Verarbeitung personenbezogener Daten in Drittländern

Version 1.2 | Auf Basis der EU-Datenschutz-Grundverordnung

www.bitkom.org

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Susanne Dehmel | Mitglied der Geschäftsleitung Vertrauen und Sicherheit
T 030 27576-223 | s.dehmel@bitkom.org

Verantwortliches Bitkom Gremium

AK Datenschutz

Satz & Layout

Kathrin Windhorst | www.kwikwi.org
Kea Schwandt | Bitkom e. V.

Titelbild

© 12521104 – istock.com

Verarbeitung personenbezogener Daten in Drittländern

Version 1.2 | Auf Basis der EU-Datenschutz-Grundverordnung

Inhaltsverzeichnis

Vorwort

»Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer« war die vierte Publikation des Bitkom-Arbeitskreises Datenschutz und stammt bereits aus dem Jahr 2005.

Der Arbeitskreis Datenschutz besteht aus Experten der Bitkom-Mitgliedsfirmen und befasst sich mit aktuellen Themen und datenschutzspezifischen Aspekten der Informations- und Kommunikationstechnik. Ein Profil des Arbeitskreises befindet sich am Ende des Leitfadens.

Die aktualisierte Version 1.1 wurde im Sommer 2016 auf Basis des noch geltenden Rechts der EU-Datenschutzrichtlinie 95/46 und des Bundesdatenschutzgesetzes sowie unter Berücksichtigung der aktuellen Rechtsprechung zu Safe Harbor erstellt. Sie diente als Orientierung für die Übergangsphase bis zur endgültigen Anwendung der EU-Datenschutz-Grundverordnung. Abrufbar auf Bitkom-Webseite: ↗https://www.bitkom.org/Bitkom/Publikationen/Uebermittlung-personenbezogener-Daten-Inland-EU-Laender-Drittlaender-2.html

Die aktuelle Version 1.2 wurde im Sommer 2017 auf Basis der EU-Datenschutz-Grundverordnung, die ab 25. Mai 2018 Anwendung findet, erstellt.

Für die letzte Aktualisierung danken wir insbesondere folgenden Mitgliedern des Arbeitskreises:

- Arnd Böken, Graf von Westphalen Rechtsanwälte
- Jonas von Dall´Armi, Vodafone Kabel Deutschland GmbH
- Frank Ingenrieth, Selbstregulierung Informationswirtschaft e. V.
- Manfred Monreal, Deutsche Post AG
- Barbara Schmitz, Osram GmbH

Zur ursprünglichen Version des Leitfadens hatten maßgeblich beigetragen: Anne Bernzen, Dr. Sibylle Gierschmann, LL. M., Ulrike Schroth, Regina Wacker-Dengler, Wolfgang Braun, Helmut Glaser, Alexander Heimel, Stefan Lerbs, Ralf Maruhn, Mirko Schmidt, Florian Thoma.

Berlin, September 2017

Als weitere Publikationen des Bitkom Arbeitskreises Datenschutz sind erhältlich:

- ↗Grafik Datenschutzkonforme Datenverarbeitung nach der EU-Datenschutz-Grundverordnung. Stand April 2017.
- ↗FAQ – Was muss ich wissen zur EU-Datenschutz Grundverordnung?
- ↗Das Safe-Harbor-Urteil des EuGH und die Folgen. Fragen und Antworten.
- ↗Mustervertragsanlage Auftragsverarbeitung und begleitende Hinweise. Stand April 2017.
- ↗Joint Controllership in der EU-Datenschutz-Grundverordnung. Checkliste. Stand April 2017.
- ↗Leitfaden Risk Assessment und Datenschutz-Folgenabschätzung. Stand April 2017.
- ↗Das Verarbeitungsverzeichnis (Version 4.0). Stand Mai 2017.

Executive Summary

Allgemein

- **Die Rahmenbedingungen für die Datenverarbeitung in Drittstaaten bleiben weitestgehend erhalten:** Die DS-GVO hält für international tätige Unternehmen die gleichen Rechtstatbestände zur Datenübermittlung in Drittstaaten wie schon die DS-RL bereit (u. a. Einwilligung, Vertrag, Standarddatenschutzklauseln (bisher: Standardvertragsklauseln), verbindliche interne Datenschutzvorschriften (Binding Corporate Rules (kurz BCR))) und teilweise neue wie genehmigte Verhaltensregeln (Codes of Conduct (kurz CoC)) und genehmigte Zertifizierungsmechanismen.

  Hinweis: Unternehmen sollten erst prüfen, ob es einen Angemessenheitsbeschluss für das Land gibt, in der der Datentransfer erfolgen soll (siehe Art. 45). Dann kann die Datenverarbeitung wie innerhalb der EU erfolgen. Falls nicht, sollte geprüft werden, ob die Datenverarbeitung unter einen gesetzlichen Ausnahmetatbestand fällt (Art. 49 DS-GVO). Ist das auch nicht der Fall muss eine geeignete Garantie gefunden oder hergestellt werden (Art. 46).

- **Stärkere ausdrückliche Einbeziehung des Auftragsverarbeiters:** Die allgemeinen Grundsätze der Datenübermittlung beziehen sich ausdrücklich auch auf Auftragsverarbeiter (Art. 44 DS-GVO). Im Allgemeinen wird der Auftragsverarbeiter für seinen Verantwortungsbereich stärker in die Pflicht genommen. Er hat eigene Dokumentationspflichten (z. B. muss er festhalten, ob und in welche Drittstaaten personenbezogene Daten übermittelt sowie welche geeigneten Garantien (Standarddatenschutzklauseln, BCRs etc.) dafür genutzt werden (Art. 30 Abs. 2 lit. c DS-GVO) und haftet bei Datenpannen unter Umständen auch direkt gegenüber dem Betroffenen (Art. 82 DS-GVO).

Datentransfer auf Basis einer Angemessenheitsentscheidung

- **Die Prüfungskriterien für Angemessenheitsentscheidungen wurden erweitert:** Die DS-GVO normiert die Prüfungskriterien für Angemessenheitsbeschlüsse, die die EU-Kommission beachten muss (Art. 45 Abs. 2 DS-GVO) wie z. B. die Rechtsstaatlichkeit, Achtung der Menschenrechte und Grundfreiheiten, wirksamer gerichtlicher Rechtsschutz und die Existenz von unabhängigen Aufsichtsbehörden. Darüber hinaus ergibt sich aus der Schrems-Entscheidung (siehe dazu Bitkom ↗FAQ Safe Harbor), dass für die Prüfung eines angemessenen Schutzniveaus u. a. auch die nationalen Vorschriften und die Praxis der Sicherheits- und Strafverfolgungsbehörden bezüglich des Zugriffs auf personenbezogenen Daten aus Gründen der öffentlichen Sicherheit in Betracht gezogen werden müssen.

  Hinweis: In der ↗EU-Mitteilung (2017) 7 hat die EU-Kommission angekündigt, dass sie sich – nach der Vereinbarung des EU-US Privacy Shields – jetzt mit den Regelungen zu Datentransfers in weitere Staaten außerhalb der EU beschäftigen wird. Geprüft wird, ob zum Beispiel andere Länder wie Japan oder Süd-Korea über ähnlich hohe Datenschutzstandards verfügen wie die EU. Diese Länder haben kürzlich neue Datenschutzgesetze erlassen und den Schutz der Privatsphäre damit gestärkt.

Datentransfer auf Basis eines gesetzlichen Ausnahmetatbestands

- **Ausnahmetatbestand des zwingenden berechtigten Interesses:** Die DS-GVO enthält eine neue Rechtsgrundlage für den einmaligen Datentransfer auf Basis zwingender berechtigter Interessen des Verantwortlichen, die allerdings nur bei außergewöhnlichen Umständen unter bestimmten Voraussetzungen genutzt werden kann, u. a. muss die Aufsichtsbehörde über den Datentransfer in Kenntnis gesetzt werden (Art. 49 Abs. 1, UAbs. 2, Abs. 6 DS-GVO).

  Beispiel: Kann beispielsweise zur Anwendung kommen, wenn Behörden in Drittstaaten (z. B. das US Department of Justice) personenbezogene Daten von in der EU ansässigen Unternehmen anfordern.

  Beispiel: Fernwartung/Trouble Support bei außergewöhnlichen Umständen (z. B. Cyberattacke) durch einen Dienstleister im Drittland, wenn Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann und der Verantwortliche keine Standardvertragsklauseln mit diesem Dienstleister abgeschlossen hat bzw. so schnell abschließen kann.

Datentransfer auf Basis einer geeigneten Garantie

- **Ausdrückliche Anerkennung BCR als geeignete Garantien:** Die DS-GVO erkennt BCR ausdrücklich als geeignete Garantien für Datentransfers in Länder ohne angemessenes Schutzniveau an (Art. 46 Abs. 2 lit. b DS-GVO). Bisher waren BCR nicht explizit in der Datenschutzrichtlinie aufgeführt. Die inhaltlichen Anforderungen von BCRs wurden von der Art. 29-Datenschutzgruppe festgelegt. Sie wurden nun weitestgehend von der DS-GVO übernommen.

- **Erweiterte Anwendung auf BCR auf Gruppen von Unternehmen, die eine gemeinsame Wirtschaftätigkeit verfolgen:** Der Kreis der möglichen Nutzer von BCR wurde deutlich erweitert. Waren BCR bislang auf eine Unternehmensgruppe (Konzern) fokussiert, stehen BCR nach der DS-GVO auch Gruppen von Unternehmen offen, die eine gemeinsame Wirtschaftstätigkeit ausüben (Art. 20 Abs. 4 DS-GVO).

  Beispiel: So können beispielweise unterschiedliche Beteiligte in der Reisebranche gemeinsam BCR verabschieden.

- **Die geeigneten Garantien werden erweitert:** Als geeignete Garantien stehen für Unternehmen neben beispielsweise Standarddatenschutzklauseln und BCR neuerdings auch genehmigte Codes of Conduct und Zertifizierungen (z. B. Datenschutzsiegel und Prüfzeichen) (Art. 46 Abs.2 lit. e und f DS-GVO) zur Verfügung.

  Beispiel: Verantwortliche außerhalb der EU können sich z. B. einem EU Code of Conduct unterwerfen oder sich einer Zertifizierung unterziehen. Dabei gehen sie die verbindliche und durchsetzbare Verpflichtung ein, sich an die Datenschutzbestimmungen zu halten, die diese Instrumente vorschreiben (siehe Art. 42 Abs. 2 DS-GVO). Dies soll die Entwicklung von

maßgeschneiderten Lösungen für internationale Datenübermittlungen ermöglichen, die z. B. die spezifischen Merkmale und Bedürfnisse für einen bestimmten Sektor oder eine bestimmte Branche oder bestimmte Datenströme widerspiegeln.

- **Standarddatenschutzklauseln als geeignete Garantien können neuerdings auch von EU-Datenschutzaufsichtsbehörden vorgeschlagen werden:** Standarddatenschutzklauseln (früher Standardvertragsklauseln) können neuerdings auch von einer EU-Aufsichtsbehörde vorgeschlagen werden. Diese sind im Kohärenzverfahren mit anderen Aufsichtsbehörden abzustimmen und bedürfen der Genehmigung der EU-Kommission, die hierfür ein EU-Prüfverfahren nach Art. 93 Abs. 1 DS-GVO anwenden muss.

  Hinweis: Laut der EU-Mitteilung COM (2017)7 arbeitet die EU-Kommission zusammen mit der Art.29–Datenschutzgruppe, die ab 2018 durch den sogenannten »Europäischen Datenschutzausschuss« ersetzt wird, derzeit an Musterdatenschutzklauseln zwischen Auftragsverarbeitern (»processor-to-processor standard contractual clauses«). Derzeit gibt es noch keine Mustervertragsklauseln zwischen Auftragsverarbeitern, sondern nur zwei unterschiedliche Sets an Klauseln für Datenübermittlungen zwischen Verantwortlichen (»controller-to-controller standard contractual clauses«) und ein Set zwischen Verantwortlichen und Auftragsverarbeitern (»controller-to-processor standard contractual clauses«).

Überblick Systematik

<table>
<tr><td colspan="6">Übermittlung in Drittstaaten nach der DS-GVO (Art. 44–49)</td></tr>
<tr><td rowspan="10">Drittstaaten mit Angemessenheitsbeschluss Art. 45</td><td colspan="5">Drittstaaten ohne Angemessenheitsbeschluss</td></tr>
<tr><td colspan="4">Datenübermittlung bei geeigneten Garantien Art. 46</td><td>Tatbestände nach Art. 49</td></tr>
<tr><td rowspan="9">BCR Art. 47 (Abs. 1b)</td><td rowspan="9">Standard-datenschutz-klauseln KOM (Abs. 1c)</td><td rowspan="9">Standard-datenschutz-klauseln DS-Aufsicht (Abs. 1d)</td><td rowspan="9">Genehmigte Verhaltensregeln n. Art. 40 (Abs. 1e)</td><td rowspan="9">Zertifizierung n. Art. 42 (Abs. 1f)</td><td>Einwilligung (Abs. 1a)</td></tr>
<tr><td>Vertrag oder vorvertragliche Maßnahmen mit dem Betroffenen o. im Interesse der betroffenen Person abgeschlossener Vertrag (Abs. 1b und c)</td></tr>
<tr><td>Übermittlung aus wichtigen Gründen des öffentlichen Interesses (Abs. 1d)</td></tr>
<tr><td>Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Abs. 1e)</td></tr>
<tr><td>Schutz lebenswichtiger Interessen (Abs. 1f)</td></tr>
<tr><td>Übermittlung aus einem Register (Abs. 1g)</td></tr>
<tr><td colspan="5">Übermittlung zur Wahrung zwingend berechtigter Interessen des Verantwortlichen erforderlich Abs. 1</td></tr>
</table>

1 Einführung: Die Übermittlung personenbezogener Daten

1 Einführung: Die Übermittlung personenbezogener Daten

Die Übermittlung personenbezogener Daten begleitet täglich die Anbahnung und Abwicklung der Geschäfte zahlreicher Unternehmen. Ebenso wie die Geschäfte macht auch die Datenübermittlung dabei schon lange nicht mehr an den Landesgrenzen Deutschlands halt, sondern erfolgt häufig grenzübergreifend zwischen europäischen Staaten oder international. Durch die ständig zunehmende Mobilität und die Globalisierung des Welthandels gewinnt dieser grenzübergreifende Datenaustausch stetig an Bedeutung. Gefördert wird dieser Trend durch die rasante informationstechnische Entwicklung: Die weltweiten Kommunikationsmöglichkeiten über miteinander verknüpfte Netze, über die mit geringem Kostenaufwand zeitnah nahezu unbegrenzt große Datenmengen ausgetauscht werden können, hat die Datenverarbeitung endgültig von ihrer räumlichen Begrenztheit befreit. Dies betrifft nicht nur den Austausch von Daten zwischen Vertragspartnern, sondern auch den Austausch und die Weitergabe im Unternehmensverbund. In internationalen Konzernen werden z. B. häufig Personaldaten zwischen den Konzerntöchtern und der Konzernholding bzw. zwischen den Tochtergesellschaften ausgetauscht. Durch die Vernetzung der Produktions- und Handelsbeziehungen bleiben personenbezogene Daten nicht nur im Unternehmen bzw. Konzern, sondern werden auch an ausländische Geschäftspartner oder internationale Datenbanken übermittelt. So ist es bspw. erforderlich, im Rahmen von Reisebuchungen Mitarbeiterdaten an eine Vielzahl Dritter weiterzugeben. Nicht zuletzt auch im Rahmen von Outsourcing-Projekten werden Daten häufig an weltweit tätige EDV-Dienstleistungsanbieter übermittelt.

Nicht immer aber sind alle Beteiligten mit den rechtlichen Anforderungen einer Datenübermittlung hinreichend vertraut. Die Anforderungen sollten jedoch von jedem Unternehmen ernst genommen werden. Eine Datenübermittlung, die nicht den gesetzlichen Voraussetzungen genügt, kann als Ordnungswidrigkeit mit Bußgeldern bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem welcher Betrag höher ist (Art. 83 Abs. 5 DS-GVO).

Vor diesem Hintergrund will die Bitkom-Publikation »Verarbeitung personenbezogener Daten in Drittländern« eine praktische Hilfestellung für den täglichen Gebrauch beim Transfer von Daten bieten. Neben einer kurzen Darstellung des Rechtsrahmens für die Datenübermittlung (Kapitel 2) wird die Datenverarbeitung in Drittstaaten mit angemessenem Datenschutzniveau (Kapitel 3) und ohne angemessenem Datenschutzniveau (Kapitel 4) aufgeführt. Die verschiedenen Konstellationen werden jeweils mit einem kurzen Fallbeispiel illustriert. Angesprochen wird auch die Datenübermittlung im Konzern (Kapitel 5). Abgerundet wird der Leitfaden schließlich durch ergänzende Materialien (Kapitel 6), Links und Literaturhinweise (Kapitel 7).

Bitte beachten Sie: Der Leitfaden kann angesichts der komplexen Materie keinen Anspruch auf Vollständigkeit erheben. Zudem ist die dargestellte Materie der fortlaufenden Entwicklung des Rechts und der Technik unterworfen. Letztlich versteht sich dieser Leitfaden daher als Einführung in die Problematik und bereitet beispielhaft Handlungsmöglichkeiten auf. Die Einbindung professioneller unternehmensinterner oder externer Berater wird dadurch jedoch nicht obsolet.

2 Rechtsrahmen

2 Rechtsrahmen

2.1 Anwendungsbereich Datenschutz-Grundverordnung

Die Datenschutzgrundverordnung (DS-GVO)(EU) 2016/679 des Europäischen Parlaments und des Rates und die Datenschutzrichtlinie (EU) 2016/680 wurden am 27. April 2016 verabschiedet und gelten ab dem 25. Mai 2018. Die DS-GVO schafft ein einheitliches Datenschutzrecht innerhalb der gesamten Europäischen Union. Als Verordnung gilt sie unmittelbar, d. h. sie braucht nicht durch nationale Gesetze umgesetzt zu werden. Dies bedeutet, dass die Datenverarbeitung in anderen EU-Ländern genauso zu behandeln ist wie innerhalb Deutschlands. Auch für die EWR-Staaten Norwegen, Island, Liechtenstein ist die Angemessenheit des Datenschutzniveaus anerkannt. Diese Länder sind bezüglich der Datenübermittlung daher mit Ländern innerhalb der EU gleichzusetzen.

Der Text der DS-GVO ist ↗hier abrufbar, in allen Amtssprachen der EU.

Die DS-GVO gilt grundsätzlich für alle Behörden der EU-Mitgliedsstaaten und für sämtliche Unternehmen der Privatwirtschaft, die eine Niederlassung innerhalb der Europäischen Union haben. Für Unternehmen ohne Niederlassung in der Union gilt sie unter bestimmten Voraussetzungen (siehe hierzu Abschnitt 2.4). Die Datenschutzrichtlinie gilt für den Polizei- und Justizbereich und bedarf eines nationalen Umsetzungsgesetzes.

Voraussetzung der Geltung ist weiter, dass personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden. Für die nichtautomatisierte Verarbeitung personenbezogener Daten gilt die DS-GVO, wenn die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DS-GVO).

2.2 Verbleibende Regelungsspielräume

Die DS-GVO will das Datenschutzrecht innerhalb der EU vereinheitlichen. Den Mitgliedsstaaten bleiben hier nur geringe Spielräume. In einigen Bereichen müssen die Mitgliedstaaten Regelungen treffen, z. B. bei der Frage welche Behörde den Mitgliedstaat im Europäischen Datenschutzausschuss repräsentiert. In anderen Bereichen, wie im Bereich des Beschäftigtendatenschutzes, können die Mitgliedstaaten in gewissen Grenzen zusätzliche bzw. ausfüllende Regelungen erlassen. Der deutsche Gesetzgeber hat am 27.04.2016 ein Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) erlassen, um verbliebende Spielräume zu nutzen und gleichzeitig die notwendige Transformation der Datenschutzrichtlinie durchzuführen. Das DSAnpUG-EU tritt gleichzeitig mit der DS-GVO im Mai 2018 in Kraft.

Der Text des DSAnpUG-EU ist ↗hier abrufbar.

In sehr geringem Umfang sieht die DS-GVO vor, dass die EU-Kommission konkretisierende Regelungen in Form von delegierten Rechtsakten schaffen kann, Art. 92 DS-GVO.

Die DS-GVO geht als EU-Verordnung dem nationalen Recht vor. Deutsche Rechtsvorschriften, die bis dahin nicht angepasst sind, sind ab Mai 2018 nicht weiter anwendbar.

2.3 Spezielle Datenschutzgesetze

Im öffentlichen Sektor sind die wichtigsten Bereiche, die durch Spezialgesetze geregelt werden, der Schutz der öffentlichen Sicherheit, die Strafverfolgung sowie der Bereich der Nachrichtendienste. Für diese Sektoren gilt die DS-GVO nicht. Für den Bereich der Strafverfolgung, der Strafvollstreckung einschließlich des Schutzes der öffentlichen Sicherheit gibt es die Richtlinie (EU) 2016/680, die insbesondere durch das DSAnpUG-EU transformiert wurde (Teil 3, §§ 45 ff.). Im Bereich der Nachrichtendienste hat die EU keine Gesetzgebungskompetenz. Hier sind allein die Mitgliedsstaaten zuständig. Auch hier nimmt das DSAnpUG-EU Änderungen an einer Vielzahl von Spezialgesetzen vor z. B. das Gesetz über den Militärischen Abschirmdienst, das Gesetz über den Bundesnachrichtendienst, das Sicherheitsüberprüfungsgesetz und das sogenannte Artikel-10-Gesetz.

Für die Wirtschaft sind die wichtigsten Bereiche, die durch Spezialgesetze geregelt werden, die Datenverarbeitung im Internet, die im Telemediengesetz geregelt wird, und die Datenverarbeitung bei der Telekommunikation, die im Telekommunikationsgesetz geregelt ist. Der EU-Gesetzgeber behandelt im Moment eine Verordnung (Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation COM (2017) 10), die diese Datenverarbeitung EU-weit einheitlich regelt. Zum Zeitpunkt dieser Veröffentlichung sind die Verhandlungen auf EU-Ebene noch nicht abgeschlossen.

Ein weiterer wichtiger Spezialbereich ist der Datenschutz im Beschäftigungsverhältnis, der weiter durch Gesetze der Mitgliedsstaaten geregelt werden kann.

2.4 Räumlicher Anwendungsbereich der DS-GVO

Der DS-GVO liegen zwei Prinzipien zu Grunde, das »Niederlassungsprinzip« und das »Marktortprinzip« (Art. 3 DS-GVO).

Die Verordnung gilt für die Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der EU. Es ist dabei unerheblich, ob die Verarbeitung in der EU stattfindet oder nicht. Eine Niederlassung ist jede feste Einrichtung von der aus eine Tätigkeit ausgeübt wird, beispielsweise von einem gemieteten Büro aus, selbst wenn die Tätigkeit nur geringfügig ist (vgl. EuGH, Urteil vom 1.10.2015, Weltimmo, C-230/14).

Beispiel: Unternehmen Inc. (U) mit Sitz in New York hat ein Büro in Berlin. Die Kundendatenbank der deutschen Filiale ist auf Servern des Unternehmens in den USA gespeichert. Die DS-GVO gilt gemäß Art. 3 Abs. 1.

Nach dem Marktortprinzip (Art. 3 Abs. 2) gilt die DS-GVO auch dann, wenn der Verantwortliche oder Auftragsverarbeiter keine Niederlassung in der Union hat, sofern Daten betroffener Personen, die sich in der Union befinden, verarbeitet werden, wenn

- den Personen Waren oder Dienstleistungen angeboten werden, auch wenn sie keine Zahlung zu leisten haben oder
- das Verhalten dieser Personen in der EU beobachtet wird.

Beispiel: Unternehmen (A) mit Sitz in China und ohne Niederlassung in Europa bietet Waren an, die auch an Käufer in Deutschland geliefert werden. Für die Datenverarbeitung gilt die DS-GVO, Art. 3 Abs. 2.

Diese Regelung gilt auch für Angebote, die unentgeltlich sind.

Beispiel: Unternehmen (F) mit Sitz in Kalifornien betreibt ein soziales Netzwerk. Das Angebot ist kostenlos, es richtet sich auch an Nutzer aus Deutschland. Die DS-GVO gilt hier.

Für die Anwendbarkeit der DS-GVO reicht es schon aus, dass das Verhalten von Nutzern aus Europa beobachtet werden soll. Da bereits das Verwenden von Cookies auf Websites der Verhaltensbeobachtung dient, ist der räumliche Anwendungsbereich der DS-GVO sehr weit. Es genügt schon, eine Website anzubieten, wenn sich diese auch an einen Nutzer aus der EU richtet.

2.5 Systematik des Datenschutzrechts

Für die Verarbeitung personenbezogener Daten gilt als allgemeiner Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt. Hier besteht ein gesetzliches Regel-Ausnahme-Verhältnis, die Verarbeitung fremder personenbezogener Daten ist regelmäßig unzulässig, soweit sie nicht ausnahmsweise erlaubt ist.

Grundsätze für die Verarbeitung personenbezogener Daten

Die DS-GVO gibt folgende Grundsätze für die Verarbeitung von personenbezogenen Daten vor (Art. 5 Abs. 1 DS-GVO):

a. Rechtmäßigkeit Verarbeitung nach Treu und Glauben, Transparenz
b. Zweckbindung
c. Datenminimierung
d. Richtigkeit
e. Speicherbegrenzung (zeitliche Begrenzung der Speicherung)
f. Integrität und Vertraulichkeit

Der Verantwortliche muss die Einhaltung dieser Grundsätze nachweisen können (»Rechenschaftspflicht«, Art. 5 Abs. 2 DS-GVO).

2.5.1 Erlaubnistatbestände

Die Verarbeitung von personenbezogenen Daten ist nur dann rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen aus Art. 6 Abs. 1 DS-GVO erfüllt ist:

a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung für einen oder mehrere bestimmte Zwecke gegeben.
b. Die Verarbeitung ist für die Erfüllung eines Vertrages mit dem Betroffenen erforderlich oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des Betroffenen erfolgen.
c. Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich; die Rechtspflicht kann sich aus dem EU-Recht oder dem Recht der Mitgliedstaaten ergeben, dem der Betroffene unterliegt.
d. Die Verarbeitung ist erforderlich, um lebenswichtige Interessen des Betroffenen oder einer anderen natürlichen Person zu schützen.
e. Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Für die Privatwirtschaft sind vor allem die Erlaubnistatbestände der Einwilligung, der Vertragserfüllung, der Erfüllung einer rechtlichen Verpflichtung sowie der Wahrung berechtigter Interessen von besonderer Bedeutung.

2.5.2 Einwilligung gemäß Artikel 7 DS-GVO

Nach der DS-GVO muss die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen. Anders als nach dem Bundesdatenschutzgesetz sieht die DS-GVO nicht mehr zwingend die Schriftform vor. Da der Verantwortliche die Einwilligung aber nachweisen muss, ist schon zu Beweiszwecken eine schriftliche Erklärung sinnvoll, diese kann auch elektronisch erfolgen. (Gem.

§36 Abs. 2 S. 3 BDSG (2018) bedarf die Einwilligung im Beschäftigungsverhältnis allerdings der Schriftform. Mehr Informationen hierzu finden Sie in 5.3.1).

Betrifft das Schriftstück noch andere Sachverhalte, wie beispielsweise in AGB, so muss die Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache eingeholt werden (Art. 7 Abs. 2). Außerdem muss sie von anderen Sachverhalten klar zu unterscheiden sein. Das erfordert beispielsweise Fettdruck oder den Abdruck in einer gesonderten Textpassage mit einem eigenen Kästchen, das der Betroffene ankreuzen muss.

Die Einwilligung muss freiwillig erteilt werden. Dabei wird auch berücksichtigt, ob der Anbieter eines Vertrages den Vertragsschluss davon abhängig gemacht hat, ob der Betroffene einer Datenverarbeitung zustimmt, die für die Erfüllung des Vertrages nicht erforderlich ist.

Insgesamt gesehen sind die Anforderungen an eine Einwilligung sehr hoch. Unternehmen sollten überprüfen, ob ihre bisher verwendeten Mustereinwilligungen den neuen Anforderungen genügen, gegebenenfalls sollten sie diese Muster bis Mai 2018 an die neuen Erfordernisse anpassen.

3 Datenverarbeitung in einem Drittland mit angemessenem Datenschutzniveau

3 Datenverarbeitung in einem Drittland mit angemessenem Datenschutzniveau

Die DS-GVO geht im Grundsatz davon aus, dass die Übermittlung von Daten an ausländische Stellen außerhalb der EU/EWR rechtmäßig nur dann erfolgen kann, wenn im Drittland ein angemessenes Datenschutzniveau gewährleistet ist.

Dieses Schutzniveau ist u. a. dann gewährleistet,

- wenn die Angemessenheit des Niveaus der Datenschutzgesetzgebung eines Landes, Gebiets oder Sektors von der EU-Kommission anerkannt ist, Art. 45.

Ist das Datenschutzniveau eines Landes nicht durch einheitliche Gesetze gesichert, kann eine Angemessenheit im Sinne des Art. 45 DS-GVO gleichwohl dann angenommen werden, wenn eine Vereinbarung des Landes mit der EU getroffen wurde, die ein angemessenes Datenschutzniveau sicherstellt und der Übermittlungsempfänger dieser Vereinbarung beigetreten ist (Beispiel: Privacy Shield der EU und den USA, dazu unter 4.7).

Information

Eine tabellarische Darstellung der Möglichkeiten der Übermittlung in Drittländer finden Sie unter Punkt 6.4!

3.1 Beurteilung der Angemessenheit

Die Feststellung der Angemessenheit erfolgt in einem förmlichen Verfahren durch die EU-Kommission (Art. 45 DS-GVO). Dieses hat sich gegenüber der Datenschutzrichtlinie 95/46/EG nicht geändert, allerdings sind die Vorschriften in vielerlei Hinsicht detaillierter:

- **Die Prüfungskriterien für Angemessenheitsentscheidungen wurden erweitert:** Die DS-GVO normiert die Prüfungskriterien für Angemessenheitsbeschlüsse, die die EU-Kommission beachten muss (Art. 45 Abs. 2 DS-GVO) wie z. B. die Rechtsstaatlichkeit, Achtung der Menschenrechte und Grundfreiheiten, wirksamer gerichtlicher Rechtsschutz und die Existenz von unabhängigen Aufsichtsbehörden. Darüber hinaus ergibt sich aus der Schrems-Entscheidung (siehe dazu Bitkom ↗FAQ Safe Harbor), dass für die Prüfung eines angemessenen Schutzniveaus u. a. auch die nationalen Vorschriften und die Praxis der Sicherheits- und Strafverfolgungsbehörden bezüglich des Zugriffs auf personenbezogene Daten aus Gründen der öffentlichen Sicherheit in Betracht gezogen werden müssen.

- **Angemessenheit nicht nur für ein Drittland, sondern auch für ein Gebiet oder ein oder mehrere spezifische Sektoren in dem Drittland:** Gem. Art. 45 Abs. 3 kann sich eine Angemessenheitsentscheidung auch auf ein Gebiet (z. B. Länder mit Föderalstruktur wie den USA)[1] oder ein oder mehrere spezifische Sektoren beziehen (z. B. private Sektor oder bestimmte Wirtschaftszweige). Dies war in der RL 95/46 EG bisher nicht vorgesehen.

Hinweis

Die Angemessenheit des Datenschutzniveaus bedeutet dabei nicht zwingend, dass die Verhältnisse gleichartig oder gleichwertig sind.

1 EU-Kommission, FAQ on Commission's adequacy finding on the Canadian Personal Information Protection and electronic Documents Act, question „Does the Commission Decision also cover provincial legislation", ↗http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/third-countries-faq/index_en.htm.

3.2 Angemessenheitsbeschlüsse

Ein angemessenes Datenschutzniveau wurde von der EU-Kommission in einer förmlichen Entscheidung für folgende Länder festgestellt:

- Argentinien (2003/490/EC)
- Andorra (2010/625/EU)
- Guernsey (2003/821/EC)
- Isle of Man (2004/411/EC)
- Jersey (2008/393/EC)
- Kanada (2002/2/EC)
- Neuseeland (2013/65/EU)
- Israel (2011/61/EU)
- Schweiz (2000/518/EC)
- Färöer Inseln (2010/146/EU)
- Uruguay (2012/484/EU)

Weitere Informationen zu den Entscheidungen der Kommission können auf der ↗EU-Datenschutz-Homepage abgerufen werden.

Beispiel: Unternehmer D mit Sitz in Deutschland übermittelt z. B. Kundendaten an das Unternehmen A mit einem angemessenen Datenschutzniveau (z. B. Schweiz, Guernsey, Argentinien, Kanada, etc.).

Angemessenheitsbeschlüsse, die die Kommission gem. Art. 25 Abs. 6 der RL 95/46 EG getroffen hat oder neue Angemessenheitsbeschlüsse auf Basis der DS-GVO bleiben in Kraft, solange bis sie durch einen Beschluss der EU-Kommission geändert, ersetzt oder aufgehoben werden. Sie unterliegen der fortwährenden Überwachung der EU-Kommission (Prüfung mindestens alle 4 Jahre), die ein Prüfverfahren einleiten muss, wenn ihr Informationen vorliegen, dass kein angemessenes Datenschutzniveau vorliegt.

3.3 Zukünftige Entwicklungen

In der ↗EU-Mitteilung (017) 7 hat die EU-Kommission angekündigt, dass sie sich mit den Regelungen zu Datentransfers in weiteren Staaten außerhalb der EU beschäftigen wird. Geprüft werden u. a. die Datenschutzregeln der wichtigsten Handelspartner in Ost- und Südostasien, zunächst Japan und Korea sowie – anhängig von Fortschritten bei der Modernisierung der Datenschutzvorschriften – mit Indien.

Mit Japan hat die EU-Kommission bereits im März 2017 einen ↗offiziellen Dialog zum Datenschutz und grenzüberschreitenden Datenverkehr aufgenommen. Am 4. Juli verkündeten die

EU-Kommissarin Věra Jourová und der Leiter der japanischen Aufsichtsbehörde Haruhi Kumazawa in einer ↗gemeinsamen Mitteilung, dass eine gegenseitige Adäquanzentscheidung bis Anfang 2018 geplant sei.

Aber auch andere Länder in Lateinamerika (Mercosur-Länder) und Länder in der Europäischen Nachbarschaft[2], die Interesse an einer Angemessenheitsfeststellung geäußert haben, werden laut EU-Kommission geprüft.

2 Die Europäische Nachbarschaftspolitik bezieht sich auf Ägypten, Algerien, Armenien, Aserbaidschan, Belarus, Georgien, Israel, Jordanien, Libanon, Libyen, Marokko, Moldau, Palästina, Syrien, Tunesien und die Ukraine.

4 Datenverarbeitung in Drittstaaten ohne angemessenes Datenschutzniveau

4 Datenverarbeitung in Drittstaaten ohne angemessenes Datenschutzniveau

4.1 Gesetzliche Ausnahmetatbestände (Artikel 49 DS-GVO)

Auch in Fällen, in denen für das betreffende Drittland kein angemessenes Datenschutzniveau festgestellt wurde, kann eine Datenübermittlung möglich sein. Art. 49 DS-GVO ermöglicht als Ausnahmevorschrift die Übermittlung in ein Drittland ohne angemessenes Datenschutzniveau. Die wichtigsten Anwendungsfälle des Art. 49 DS-GVO, u. a. Übermittlung zur Vertragserfüllung, Einwilligung des Betroffenen, werden in diesem Abschnitt erläutert.

4.1.1 Zur Vertragserfüllung notwendige Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau

Eine Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau ist ausnahmsweise zulässig, wenn zwischen dem Betroffenen und dem Verantwortlichen ein Vertrag abgeschlossen worden ist, für dessen Erfüllung die Datenübermittlung erforderlich ist, Art. 49 Abs. 1 S. 1 lit. b. Das gilt auch dann, wenn die Übermittlung zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist.

Der praktische Anwendungsbereich dieser Zulässigkeitsalternative liegt neben dem internationalen Zahlungsverkehr und Kaufverträgen im Fernabsatz vor allem im Tourismusgewerbe. Die Durchführung von vertraglichen Vereinbarungen über internationale Beförderungsleistungen, Reservierungen von Mietwagen, Unterkünften oder Hotelzimmern in Drittländern wird so ermöglicht.

Beispiel: Kunde (K) möchte, dass sein Reisebüro für ihn in Peking ein Hotelzimmer reserviert. Das Reisebüro kann sich für die Übermittlung der Daten des (K) an das Hotel in Peking auf Art. 49 Abs. 1 S. 1 lit b) DS-GVO berufen, da zur Durchführung bzw. Erfüllung des Vertrages zwischen Kunde (K) und dem Reisebüro die Weitergabe seiner Daten zwingend notwendig ist.

Ein Vertrag i.S.d. lit. b kann auch ein Arbeitsvertrag sein, so dass die Übermittlung von Arbeitnehmerdaten in ein Drittland auf Grund eines Arbeitsvertrages zulässig sein kann. Entscheidend für die Beurteilung der Zulässigkeit ist, ob die Übermittlung für die Durchführung bzw. Erfüllung der jeweiligen einzelnen Regelung des Arbeitsvertrags erforderlich ist. Dies ist für jeden Arbeitnehmer gesondert zu prüfen. Denkbar ist die Zulässigkeit der Datenübermittlung z. B., wenn der Mitarbeiter zu Auslandseinsätzen verpflichtet ist oder bei der Gewährung von Aktienbezugsrechten, die in einem Drittland verwaltet werden.

Hinweis

Die Voraussetzungen für eine rechtmäßige Übermittlung im Inland gemäß Art. 6 DS-GVO sind auch bei einer Datenübermittlung in ein Drittland relevant, denn bei jeder Datenübermittlung ins Ausland muss neben der Frage nach den speziellen Voraussetzungen für die Übermittlung in ein bestimmtes Land zusätzlich geprüft werden, ob darüber hinaus auch die allgemeinen Voraussetzungen für eine Übermittlung vorliegen

Erforderlich ist also eine ZWEISTUFIGE PRÜFUNG.

Etwas anders ist es bei der Konstellation, für die Art. 49 Abs. 1 S. 1 lit. c die Zulässigkeit einer Datenübermittlung begründen kann. Nach lit. c kann eine Übermittlung zulässig sein, die zur Erfüllung eines Vertrags notwendig ist, der zwar nicht vom Betroffenen selbst mit dem Verantwortlichen geschlossen wurde, aber im Interesse des Betroffenen zwischen dem Verantwortlichen und einem Dritten.

Beispiel: Der Arbeitgeber übermittelt Daten eines Arbeitnehmers, für den er eine Mitarbeiterversicherung abgeschlossen hat, an eine ausländische Versicherungsgesellschaft. Häufig wird es sich bei der Anwendung von lit. c) um Verträge zugunsten Dritter i.S.d. § 328 BGB handeln.

4.1.2 Datenübermittlung auf der Grundlage einer Einwilligung

Wie bei der Datenübermittlung innerhalb Deutschlands oder innerhalb der EU/EWR kann auch eine Datenübermittlung in ein Drittland auf der Grundlage einer Einwilligung des Betroffenen zulässig sein, Art. 49 Abs. 1 S. 1 lit. a DS-GVO.

Für die Einwilligung in die Drittlandübermittlung von Daten gelten die schon in Punkt 2.4.2 dargestellten, strengen Anforderungen.

Beim Datentransfer in ein Drittland kommt noch eine weitere Schwierigkeit hinzu. Denn nach Art. 49 Abs. 1 S. 1 lit. a DS-GVO ist der Betroffene (zusätzlich zu den oben aufgeführten Umständen der Datenübermittlung) umfassend über die Risiken der Übermittlung seiner Daten in ein Land ohne ausreichendes Datenschutzniveau zu informieren. Erforderlich ist also die Transparenz bezüglich der Schutzmaßnahmen bzw. Datenschutzgarantien bei der empfangenden Stelle oder im Empfängerland.

4.1.3 Datenübermittlung auf Grund zwingender berechtigter Interessen

Für eng umgrenzte Ausnahmefälle gestattet Art. 49 Abs. 1 S. 2 DS-GVO eine Übermittlung in einen Drittstaat ohne angemessenes Datenschutzniveau. Danach ist die Übermittlung zulässig, wenn sie nur einmal erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, die Interessen oder die Rechte und Freiheiten der betroffenen Personen nicht überwiegen und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Zusätzlich hat der Verantwortliche die Aufsichtsbehörde sowie die betroffenen Personen zu informieren. Die Beurteilung sowie die angemessenen Garantien sind in das Verarbeitungsverzeichnis nach Art. 30 DS-GVO aufzunehmen.

Der Anwendungsbereich dieser Ausnahmevorschrift ist sehr eng. In ErwG. 113 werden als Beispiele wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke genannt. Sofern

eine Übermittlung auf diesen Ausnahmetatbestand gestützt werden soll, ist es dem Verantwortlichen anzuraten, schon vorab Kontakt zur zuständigen Aufsichtsbehörde aufzunehmen.

4.1.4 Datenübermittlung in ein Drittland auf Anweisung eines Gerichts oder einer Behörde

Anders als die RL 95/46 EG enthält die DS-GVO eine ausdrückliche Regelung der Fälle, in denen ein Gericht oder eine Behörde eines Drittlandes die Übermittlung personenbezogener Daten verlangt.

Art. 48 DS-GVO bestimmt, dass diese Urteile oder Verwaltungsentscheidungen in der EU nur dann anerkannt und befolgt werden dürfen, wenn sie auf ein Rechtshilfeabkommen oder eine andere internationale Übereinkunft zwischen dem Drittland und der EU oder dem Mitgliedsstaat gestützt sind. Das können bspw. das »Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen« sein oder auch internationale Übereinkünfte im Bereich der Zusammenarbeit bei der Verbrechensbekämpfung und der Strafverfolgung.

Sofern das Gerichtsurteil oder die Verwaltungsentscheidung nicht auf ein Rechtshilfeabkommen oder eine sonstige internationale Übereinkunft gestützt werden kann, können sie die Datenübermittlung nicht rechtfertigen. Dann gelten die allgemeinen Grundsätze: Nur wenn eine gesetzliche Erlaubnis für eine Übermittlung vorliegt und im Empfängerland ein angemessenes Schutzniveau besteht oder eine Ausnahme nach Art. 49 DS-GVO gegeben ist, ist eine Übermittlung zulässig.

4.2 Garantien – Einführung

Bei Fehlen eines Angemessenheitsbeschlusses können geeignete Garantien für den Schutz der Betroffenen den im Drittland bestehenden Mangel an Datenschutz ausgleichen. Hierbei unterscheidet Art. 46 DS-GVO zwischen genehmigungsfreien Garantien (Abs. 2) und genehmigungspflichtigen Garantien (Abs. 3).

Garantien ohne besondere Genehmigung der Aufsichtsbehörden können bestehen in:

a. einem rechtlich bindenden und durchsetzbaren **Dokument zwischen den Behörden oder öffentlichen Stellen**,
b. verbindlichen internen **Datenschutzvorschriften gemäß Art. 47**,
c. **Standarddatenschutzklauseln,** die von **der Kommission** gemäß dem Prüfverfahren nach Art. 93 Abs. 2 erlassen werden,
d. **von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln**, die von der Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 genehmigt wurden,
e. genehmigten **Verhaltensregeln gemäß Art. 40** zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder

f. einem genehmigten **Zertifizierungsmechanismus gemäß Art. 42** zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

Zu den Garantien, die gem. Art. 46 Abs. 3 DS-GVO dem Vorbehalt der Genehmigung der zuständigen Aufsichtsbehörde unterliegen, gehören

a. **Vertragsklauseln**, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, und
b. **Bestimmungen**, die **in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen** aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen.

Zweck der Garantien ist die angemessene Beachtung der Datenschutzvorschriften und Rechte der betroffenen Personen.

4.3 Standarddatenschutzklauseln, Art. 46 Abs. 2 lit. c und d DS-GVO

Gem. Art. 46 Abs. 2 DS-GVO können Datenübermittlungen an ein Drittland auch auf Standarddatenschutzklauseln der Kommission (lit. c) oder der Aufsichtsbehörde (lit. d) gestützt werden. Zwar ist auch diese Möglichkeit bereits in der RL 95/46 EG in Art. 26 Abs. 4 verankert RL 95/46/EG, doch kennt die Richtlinie sie nur in der Variante, die von der Kommission als »Standardvertragsklauseln« verabschiedet werden. Die DS-GVO sieht zusätzlich vor, dass auch Aufsichtsbehörden Standarddatenschutzklauseln entwickeln können, welche von der Kommission im Rahmen eines Prüfverfahrens genehmigt werden müssen.

Hinweis

Während Art. 26 Abs. 4 der RL 95/46/EG von **Standardvertragsklauseln** spricht, bezeichnet die DS-GVO in Art. 46 Abs. 2 sowie im EG 108 die von der Kommission oder einer Aufsichtsbehörde vorgegebenen Garantien zum Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz nunmehr als **Standarddatenschutzklauseln**.

Basierend auf Art. 26 Abs. 4 der RL 95/46 EG hatte die Kommission Standardvertragsklauseln für unterschiedliche Fallkonstellationen verabschiedet:

- Standardvertragsklauseln für die Datenübermittlung zwischen für die Verarbeitung Verantwortlichen (Controller-Controller-Transfer)
  - Set I aus der Entscheidung 2001/497/EG vom 15. Juni 2001
  - Set II (sog. alternative Standardvertragsklauseln) aus der Entscheidung 2004/915/EG vom 27. Dezember 2004 zur Änderungen der Entscheidung 2001/497/EG
- Standardvertragsklauseln für die Datenübermittlung zwischen für die Verarbeitung Verantwortlichen und nach deren Weisung handelnden Auftragsverarbeitern (Controller-Processor-Transfer):

- Beschluss 2010/87/EU vom 5. Februar 2010 (die früheren Standardvertragsklauseln zur Auftragsverarbeitung aus der Entscheidung 2002/16/EG vom 27. Dezember 2001 gelten nur für vor dem 15.05.2010 geschlossene Verträge)

Während für Datenübermittlungen zwischen verantwortlichen Stellen und ihren Auftragsverarbeitern somit lediglich ein Typ an Standarddatenschutzklauseln existiert, besteht bei Datenübermittlungen zwischen verantwortlichen Stellen die Wahlmöglichkeit aus zwei Sets. Diese unterscheiden sich insbesondere hinsichtlich der Haftung, Bindung an aufsichtsbehördliche Hinweise bzw. Entscheidungen und die Gestaltungs- bzw. Ergänzungsspielräume. Allerdings ist das Set II aufgrund der eingeschränkten Haftung und Auskunftspflicht des Datenexporteurs und den hieraus resultierenden Wertungswidersprüchen zum deutschen Recht grundsätzlich nicht geeignet für die Übermittlung von Beschäftigtendaten.[3] Das Set II wurde von der Internationalen Handelskammer unter Beteiligung weiterer Wirtschaftsverbände mit der Kommission ausgehandelt, um Schwächen der Standardvertragsklauseln von Juni 2001 auszugleichen. Diese »alternativen Klauseln« werden daher von vielen Unternehmen insgesamt als vorzugswürdig eingestuft.

Set I (2001/497/EG vom 15.6.2001)	Set II (2004/915/EG vom 27.12.2004), alternative Klauseln
Gesamtschuldnerische Haftung *vgl. Klausel 6*	Jede Partei haftet für eigenes Verschulden; Strafschadenersatzansprüche (punitive damages) sind ausgeschlossen; *vgl. Ziffer III* Aber: wegen Haftungseinschränkung grundsätzlich nicht geeignet für Beschäftigtendaten
strengere Bindung an (unverbindliche) Ratschläge (»advice«) der Aufsichtsbehörden *vgl. Klausel 5*	Bindung an bestandskräftige (verbindliche) Entscheidungen (»decisions«) der Aufsichtsbehörden; *vgl. Ziffer V*
Klauseländerungsverbot *vgl. Klausel 11*	Erlaubnis für ergänzende Verträge zur Regelung kommerzieller Fragen; Beschreibung der Übermittlung in Anhang B, kann angepasst und ergänzt werden; *vgl. Ziffer VII*

Bei der Verwendung von Standarddatenschutzklauseln ist darauf zu achten, dass die vorgegebenen Klauseln von den Vertragspartnern grundsätzlich nicht verändert oder durch Nebenabreden anderweitig eingeschränkt werden dürfen. Ergänzungen sind nur im Rahmen sog. geschäftlicher Klauseln zulässig, soweit die betreffenden Standarddatenschutzklauseln eine solche Ergänzung zulassen und solange diese nicht direkt oder indirekt im Widerspruch zu den Standarddatenschutzklauseln stehen oder Grundrechte oder Grundfreiheiten der betroffenen Personen verletzen. Im Fall einer unzulässigen Änderung verlieren die Klauseln ihren privilegierten Status als Standarddatenschutzklauseln im Sinne des Art. 46 Abs. 2 DS-GVO und unterliegen sodann als »einfache« Vertragsklauseln der Genehmigungspflicht. Erfolgt die Übermittlung hingegen auf Basis von (unveränderten) Standarddatenschutzklauseln bedarf es nach deutschem Datenschutzrecht hingegen keiner Genehmigung durch die Aufsichtsbehörde, da die Kommission im Rahmen des Prüfverfahrens nach Art. 93 Abs. 2 DS-GVO (bzw. nach Art. 26 Abs. 4 i. V.m. Art. 31

Hinweis

In anderen EU-Staaten (z. B. AT, HR, CY, EE, FR, IS, LV, LT, LU, MT, RO, SI, ES) konnte bisher unter der Datenschutzrichtlinie eine Genehmigung auch im Fall von Standardvertragsklauseln erforderlich sein. Dies ist nach der DS-GVO in allen EU-Staaten nun nicht mehr erforderlich.

3 Vgl. Abgestimmte Positionen der Aufsichtsbehörden in der AG »Internationaler Datenverkehr« am 12./13. Februar 2007, Seite 2, II.2.

Abs. 2 der RL 95/46 EG) ja bereits die Feststellung getroffen hat, dass die Standarddatenschutzklauseln ausreichende Garantien zum Schutz der Persönlichkeitsrechte der Betroffenen enthalten. Allerdings können Aufsichtsbehörden die Vorlage der vereinbarten Standarddatenschutzklauseln verlangen.[4]

Exkurs: Anwendbarkeit der Standardvertragsklauseln nach dem EuGH-Urteil zu Safe Harbor vom 6.10.2015

Mit der Angemessenheitsentscheidung »Safe Harbor« hatte die EU-Kommission die Voraussetzung geschaffen, ein angemessenes Datenschutzniveau im Sinne von Art. 25. Abs. 2 DS-RL für den Transfer personenbezogener Daten in die USA anzunehmen, wenn sich der Importeur in den USA den Safe-Harbor-Prinzipien und den sog. »Frequently Asked Questions« unterwirft. Diese Entscheidung hat der EuGH mit seiner Entscheidung vom 6. Oktober 2015 (sog. »Schrems-Urteil«) jedoch für unwirksam erklärt. Mit der Folge, dass der Datentransfer in die USA auf der Grundlage der Safe Harbor-Feststellung spätestens seit Ende Januar 2016 nicht mehr zulässig ist (siehe dazu ↗Positionspapier der Datenschutzkonferenz und ↗der Art. 29 Datenschutzgruppe).

Nach überwiegender Auffassung der Aufsichtsbehörden, der Literatur und der EU-Kommission haben Standarddatenschutzklauseln mit dem EuGH-Urteil nicht per se ihre Gültigkeit verloren und können daher bis auf weiteres weiterverwendet werden. Insbesondere obliegt die Befugnis, eine Entscheidung der Kommission über Standarddatenschutz- bzw. -vertragsklauseln für unwirksam zu erklären, allein dem EuGH (Vgl. EuGH, Urteil vom 6.10.2015, Schrems, C-362/14, RZ 61). Solange eine solche Feststellung nicht vorliegt, ist die Entscheidung der Kommission nach Art. 288 Abs. 4 AEV für alle Organe der Mitgliedstaaten verbindlich (Vgl. EuGH, Urteil vom 6.10.2015, Schrems, C362/14, RZ 51).

Gleichwohl ist die Frage der Gültigkeit bzw. Vereinbarkeit der bestehenden Standardvertragsklauseln mit europäischem Recht weiterhin Gegenstand gerichtlicher Verfahren und Diskussionen. So setzt sich der irische High Court in einem weiteren Prozess (auch als Schrems II bezeichnet) mit der Datenübermittlung von Facebook in die USA auseinander, wobei die irische Datenschutzbeauftragte generell die Frage der Legitimation von Datenübermittlungen in Drittländer durch Standardvertragsklauseln durch den EuGH klären lassen möchte (vgl. Irish High Court, Schrems II, Az. 2016/4809P). Die Anhörungen der im Prozess involvierten Parteien fanden von Juli 2016 bis Januar 2017 statt. Die Entscheidung darüber, ob der irische Gerichtshof die von der irischen Aufsichtsbehörde offenen Fragen dem EuGH vorlegt, steht derzeit noch aus. Mehr Informationen zu diesem Verfahren finden Sie auf der ↗Webseite der irischen Datenschutzaufsichtsbehörde.

4 Weiterführend zum Thema Standardvertragklauseln Schmitz/v. Dall'Armi, ZD 2016, 217ff.

4.4 Individuelle Vertragsklauseln, Art. 46 Abs. 3 lit. a DS-GVO

Der Datenexporteur, der sowohl Verantwortlicher oder Auftragsverarbeiter sein kann, kann mit dem im Drittland ansässigen Verantwortlichen, Auftragsverarbeiter oder Empfänger einen individuellen, d. h. selbst formulierten Vertrag zum Datenschutz schließen, welcher von der zuständigen Aufsichtsbehörde – bei Post- und Telekommunikationsunternehmen durch den/die Bundesbeauftragte(n) für den Datenschutz und die Informationsfreiheit (BfDI) – genehmigt werden muss. Diese Möglichkeit der Umsetzung angemessener Garantien kannte bereits die RL 95/46 EG in Art. 26 Abs. 2.

4.5 Verbindliche interne Datenschutzvorschriften (»Binding Corporate Rules«)

4.5.1 Einleitung

Der europäische Gesetzgeber hat »verbindliche interne Datenschutzvorschriften«, so die offizielle deutschsprachige Bezeichnung für »Binding Corporate Rules«, explizit in den Kreis der »geeigneten Garantien« zur Absicherung von Datenverarbeitungen in Ländern ohne angemessenes Schutzniveau aufgenommen, Art. 46 Abs. 2 lit. b DS-GVO. »Geeignete Garantien« sollen eine Kompensation dafür schaffen, dass personenbezogene Daten in einem Land verarbeitet werden, das über kein (festgestelltes) adäquates Datenschutzniveau verfügt, ErwG. 108. Ziel ist die weitestgehende Gewährleistung, dass personenbezogene Daten auch dort gemäß den Prinzipien der DS-GVO verarbeitet werden und Betroffene ihre gesetzlich normierten Rechte durchsetzen können.

Beachten!

»Geeignete Garantien« bezwecken – nur – einen Ausgleich für den Transfer von personenbezogenen Daten in »unsichere Drittländer«. Deshalb müssen bei der Verarbeitung der personenbezogenen Daten stets – auch – die allgemeinen Anforderungen an eine rechtskonforme Datenverarbeitung erfüllt werden. Dies stellt ErwG. 48 in Satz 2 klar! Eine Verarbeitung personenbezogener Daten bedarf daher stets einer sie legitimierenden Grundlage im Sinne von Art. 6 Abs. 1 DS-GVO und auch bei konzerninternen Auftragsverarbeitungen ist immer ein Vertrag gemäß Art. 28 DS-GVO zu schließen (siehe hierzu auch 5.4).

Die DS-GVO hat weitestgehend die von der Art. 29-Datenschutzgruppe (Datenschutzgruppe) entwickelten inhaltlichen Anforderungen an BCR übernommen, die diese im Laufe der letzten zwanzig Jahre in mehreren Arbeitspapieren (Working Paper, kurz »WP« genannt und durchlau-

fend nummeriert) veröffentlicht hat.5 Rechtsdogmatisch betrachtet sind BCR weder ein Vertrag noch Verhaltensregeln, sondern ein Instrument der »Selbstkontrolle der Wirtschaft« (WP 12). BCR waren dadurch gekennzeichnet, dass sie verbindlich bzw. rechtlich durchsetzbar, unternehmensintern und für internationale Datentransfers bestimmt sind (WP 74). Zentrales Element war die einseitige Selbstverpflichtungserklärung der Unternehmungsleitung, die Grundsätze des europäischen Datenschutzrechts bei Verarbeitungen außerhalb der Europäischen Union zu beachten. Die Selbstverpflichtungserklärung ist aber auch ein gewisses Manko, weil sie als einseitige Willenserklärung nicht in allen Rechtsordnungen als rechtsverbindlich angesehen wird (WP 74). Dieses Akzeptanzproblem dürfte sich durch die ausdrückliche Aufnahme in der DS-GVO zumindest für die Mitgliedstaaten der EU erledigt haben. Während Standardvertragsklauseln einmalig Übermittlungen an individuelle Empfänger absichern, stellen BCR eine dauerhafte Absicherung für unzählige Übermittlungen an einen oder mehrere Empfänger dar. Aus diesen Besonderheiten leiten sich spezielle Anforderungen (siehe 4.5.3) ab, die interessierte Nutzer erfüllen müssen.

4.5.2 Begriff

Verbindliche interne Datenschutzvorschriften sind gemäß der Legaldefinition in Art. 4 Abs. 20 DS-GVO »Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern«.

Damit hat sich der Gesetzgeber vom Konzept der »unternehmensinternen« Regeln verabschiedet und BCR zu »internen« Regeln für Unternehmen gemacht, die ggfs. keine gemeinsame steuernde »Unternehmensführung« haben.

4.5.3 Anforderungen

Art. 47 DS-GVO enthält eine lange Liste von Anforderungen, die BCR erfüllen müssen. Viele der Anforderungen sind vage formuliert und lassen Raum zur Interpretation. Bei der Auslegung der Anforderungen werden die Aufsichtsbehörden auf ihre in den letzten Jahren veröffentlichten Arbeitspapiere zurückgreifen, in denen teilweise sehr präzise Aussagen zur Verwirklichung einzelner Anforderungen gemacht wurden. Das WP 153 enthält Aussagen darüber, welche Anforderungen in den BCR zu erfüllen sind und wo man weitere Informationen zu den Anforderungen finden kann. Die Darstellung versucht hierzu einen Überblick zu geben.

5 Insbesondere die WP 12, 74, 108, 153, 155.

Anforderung	In BCR zu erfüllen?	Anmerkung
Abs. 1 lit. a BCR sind für alle betreffenden Mitglieder der Unternehmensgruppe bzw. Gruppe von Unternehmen verbindlich und werden durchgesetzt, und zwar auch für ihre Beschäftigten,	Ja	WP 153 Punkt 1.1 und 1.2
Abs. 1 lit. b Betroffenenrechte haben drittbegünstigende Wirkung	Ja	WP 153 Punkt 1.3
Abs. 2 lit. a Struktur und Kontaktdaten der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und jedes ihrer Mitglieder;	Nein	WP 153 Punkt 6.2
Abs. 2 lit. b die betreffenden Datenübermittlungen oder Reihen von Datenübermittlungen einschließlich der betreffenden Arten personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;	Ja	WP 153 Punkt 4.1
Abs. 2 lit. c interne und externe Rechtsverbindlichkeit der betreffenden internen Datenschutzvorschriften;	Ja	WP 153 Punkt 1.1 und 1.2
Abs. 2 lit. d die Anwendung der allgemeinen Datenschutzgrundsätze, insbesondere Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rechtsgrundlage für die Verarbeitung, Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und Anforderungen für die Weiterübermittlung an nicht an diese internen Datenschutzvorschriften gebundene Stellen;	Ja	WP 153 Punkt 6.1
Abs. 2 lit. e die Rechte der betroffenen Personen in Bezug auf die Verarbeitung und die diesen offenstehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung nach Art. 22 unterworfen zu werden sowie des in Art. 79 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde bzw. auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen internen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;	Ja	WP 153 Punkt 1.3
Abs. 2 lit. f die von dem in einem Mitgliedstaat niedergelassenen Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße eines nicht in der Union niedergelassenen betreffenden Mitglieds der Unternehmensgruppe gegen die verbindlichen internen Datenschutzvorschriften; der Verantwortliche oder der Auftragsverarbeiter ist nur dann teilweise oder vollständig von dieser Haftung befreit, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;	Ja	WP 153 Punkt 1.6
Abs. 2 lit. g die Art und Weise, wie die betroffenen Personen über die Bestimmungen der Art. 13 und 14 hinaus über die verbindlichen internen Datenschutzvorschriften und insbesondere über die unter den Buchstaben d), e) und f) genannten Aspekte informiert werden;	Ja	WP 153 Punkt 1.7 Die Mitglied-staaten können bei die Nutzung von BCR für Beschäftig-ten-daten besonde-re Transparenzan-forderungen aufstellen, Art 88 Abs.2 DS-GVO.

Anforderung	In BCR zu erfüllen?	Anmerkung
Abs. 2 lit. h die Aufgaben jedes gemäß Art. 37 benannten Datenschutzbeauftragten oder jeder anderen Person oder Einrichtung, die mit der Überwachung der Einhaltung der verbindlichen internen Datenschutzvorschriften in der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sowie mit der Überwachung der Schulungsmaßnahmen und dem Umgang mit Beschwerden befasst ist;	Ja	WP 153 Punkt 2.4
Abs. 2 lit. i die Beschwerdeverfahren;	Ja	WP 153 Punkt 2.2
Abs. 2 lit. j die innerhalb der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen internen Datenschutzvorschriften. Derartige Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Abhilfemaßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse derartiger Überprüfungen sollten der in Buchstabe h) genannten Person oder Einrichtung sowie dem Verwaltungsrat des herrschenden Unternehmens einer Unternehmensgruppe oder der Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, mitgeteilt werden und sollten der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden;	Ja	WP 153 Punkt 2.3
Abs. 2 lit. k die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;	Ja	WP 153 Punkt 5.1
Abs. 2 lit. l die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gewährleisten, insbesondere durch Offenlegung der Ergebnisse von Überprüfungen der unter Buchstabe j) genannten Maßnahmen gegenüber der Aufsichtsbehörde;	Ja	WP 153 Punkt 3.1
Abs. 2 lit. m die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken könnten, die die verbindlichen internen Datenschutzvorschriften bieten;	Ja	WP 153 Punkt 6.3
Abs. 2 lit. n geeignete Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten.	Ja	WP 153 Punkt 2.1

Überlegung!

Diese von der Datenschutzgruppe über viele Jahre entwickelten und aufgestellten Anforderungen beruhen auf der Prämisse, dass sie für einen Unternehmensverbund mit einer zentralen und steuernden Stelle gelten. Durch die Erweiterung der Nutzergruppe und die teilweise fehlende Akzeptanz von BCR in einigen Rechtsordnungen, kann es eine Überlegung für Interessierte sein, ihre BCR als multilateralen Vertrag auszugestalten.

Tipp!

Die Arbeitspapiere der Datenschutzgruppe sind auch nach dem 25. Mai 2018 gültig und enthalten viele interessante Erläuterungen. Besonders hinzuweisen ist auf die WP 74 und WP 108 sowie auf das WP 155, das eine FAQ-Liste zu BCRs enthält. Diese wird bei Bedarf aktualisiert; letztmalig im Februar 2017(rev.05).

4.5.4 Genehmigungsverfahren

BCR sind von der zuständigen Aufsichtsbehörde nach dem Kohärenzverfahren zu genehmigen, Art. 57 Abs. 1 lit. s, Art. 47 Abs. 1 i. V.m. Art. 64 Abs. 1 lit. f DS-GVO. Hierdurch soll gewährleistet werden, dass die europäischen Aufsichtsbehörden aufgrund eines gemeinsamen Verständnisses eine von allen getragene Entscheidung herbeiführen und so einen Beitrag zur einheitlichen Anwendung der DS-GVO leisten.

Das DSAnpUG-EU hat in § 19 Abs. 1 BDSG (2018) festgelegt, dass die Behörde die federführende Behörde ist, in deren Land der Verantwortliche oder der Auftragsverarbeiter seine Hauptniederlassung hat. In Anlehnung an die europarechtlichen Vorgaben ist in § 18 BDSG (2018) das Verfahren der Zusammenarbeit der Behörden des Bundes und der Länder dezidiert geregelt worden.

Der Gesetzgeber hat der bisherigen Praxis ein Ende bereitet, nach der einzelne oder – im Falle des Verfahrens der gegenseitigen Anerkennung – drei nationale Aufsichtsbehörden aufgrund ihres individuellen Verständnisses eine Entscheidung über die Rechtmäßigkeit der vorgelegten BCR getroffen haben. Die Erfahrung mit den oftmals sehr langen Genehmigungsverfahren hat dazu geführt, dass es nunmehr gesetzliche Fristen gibt, die das Verfahren beschleunigen werden. Positiv ist in diesem Zusammenhang auch zu werten, dass das Schweigen einer in das Genehmigungsverfahren eingebundenen Aufsichtsbehörde als Zustimmung gewertet wird, Art. 64 Abs. 3 DS-GVO.

Werden von den Aufsichtsbehörden genehmigte BCR als Absicherung für Drittlandtransfers genutzt, bedarf es keiner weiteren »besonderen Genehmigung einer Aufsichtsbehörde«, Art. 46 Abs. 2 1. Halbsatz DS-GVO. Damit hat der europäische Gesetzgeber einer von einigen Aufsichtsbehörden gepflegten Praxis jede Grundlage entzogen und so einen aktiven Beitrag zur harmonisierten Datenschutzpraxis geleistet.

4.5.5 »Alt-BCR«

Art. 46 Abs. 5 DS-GVO stellt klar, dass die von Aufsichtsbehörden auf der Grundlage von Art. 26 Abs. 2 RL 95/46 EG erteilten Genehmigungen so lange gültig bleiben, bis sie aufgehoben werden. Somit sind genehmigte (Alt-) BCR grundsätzlich auch nach dem 25. Mai 2018 gültig und können zur Absicherung von internationalen Datentransfers genutzt werden.

(Alt-)BCR spiegeln allerdings die datenschutzrechtliche Situation unter Geltung der RL 95/46 EG bzw. der darauf erlassenen nationalen Datenschutzgesetze wider. Auch wenn die Regelungen zur »Übermittlung personenbezogener Daten in Drittländer«[6] inhaltlich von der DS-GVO übernommen wurden, dürfte sich bezüglich anderer Fragestellungen ein gewisser Anpassungsbedarf ergeben. Werden der zuständigen Aufsichtsbehörde die geänderten BCR vorgelegt, stellt dies eine Änderungsmeldung gemäß Art. 47 Abs. 2 lit. k DS-GVO und nicht einen Antrag auf Genehmigung von (neuen) BCR dar.

4.6 Genehmigte Verhaltensregen (»Codes of Conduct«) oder Zertifizierung

Mit der Datenschutz-Grundverordnung werden zwei neue Typen von geeigneten Garantien eingeführt.

4.6.1 Genehmigte Verhaltensregeln

Art. 46 Abs. 2 lit. e DS-GVO nennt genehmigte Verhaltensregeln nach Art. 40 DS-GVO als geeignete Garantien, wenn sie zusammen gehen mit rechtlich durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland, diese Garantien auch anzuwenden – inklusive der Betroffenenrechte. Dafür können nach Art. 40 Abs. 3 DS-GVO Verantwortliche oder Auftragsverarbeiter im Drittland mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung eingehen, die geeigneten Garantien anzuwenden. Es bedarf also neben den durch die Aufsichtsbehörden genehmigten Verhaltensregeln eines Aktes des Unternehmens, der eine Durchsetzung der Garantien im Drittland für Betroffene ermöglicht. Die Einhaltung muss für die Betroffenen rechtlich durchsetzbar sein – dazu muss es wirksame Rechtsbehelfe geben (wie gerichtliche Rechtsbehelfe sowie das Recht auf Geltendmachung von Schadenersatzansprüchen).

4.6.1.1. Erforderlichkeit

Betrachtet man die Angriffe der bestehenden Rechtfertigungsmechanismen in den letzten Jahren (Safe Harbour oder aktuell Standarddatenschutzklauseln), so kann festgehalten werden: einen Drittstaatentransfer lediglich auf einen der möglichen Rechtfertigungstatbestände zu stützen ist riskant. Der Europäische Gerichtshof hat mit seinem Urteil zu Safe Harbour zudem deutlich gemacht: es gibt keine Garantie für eine Übergangsphase. Theoretisch kann eine Rechtfertigung ad hoc und von einen Tag auf den anderen wegfallen.

6 So der Titel von Kapitel IV der RL 95/46 EG.

4.6.1.2 Umsetzungsmöglichkeiten

Betrachtet man Verhaltensregeln in der Gesamtschau bestehender Rechtfertigungsmöglichkeiten, so dürfen die Anforderungen nicht zu hoch angesetzt werden. Hierbei ist auch zunächst zu beachten, wie hoch die Anforderungen an eine Anerkennung nach Art. 40 DS-GVO sind.

4.6.1.2.1 Hintergrund

Verhaltensregeln sind nur anerkennungsfähig, wenn diese aus Sicht der Aufsichtsbehörden zur ordnungsgemäßen Anwendung der DS-GVO beitragen, z. B. durch eine Präzisierung der Anwendung der DS-GVO. Ergänzend müssen Verhaltensregeln vorsehen, dass eine unabhängige Aufsichtsstelle die Einhaltung der Verhaltensregeln durch jene überwacht, die sich den Verhaltensregeln unterworfen haben und sich letztlich auf die Rechtswirkungen der Verhaltensregeln berufen möchten.

Hierdurch ergibt sich bereits, dass Verhaltensregeln kein Selbstzweck sind. Verhaltensregeln im Sinne der DS-GVO sind als glaubwürdige und seriöse Ergänzung zur staatlichen Aufsicht zu verstehen. So hat die unabhängige Aufsichtsstelle zwingend ein Beschwerdeverfahren vorzusehen. Die unabhängige Aufsichtsstelle ist zudem mit hinreichenden Sanktionsmöglichkeiten auszustatten und ist gegenüber der Datenschutzaufsicht selbst berichtspflichtig. Hierdurch besteht nicht nur die Möglichkeit durch die staatliche Aufsicht korrigierend einzugreifen. Vielmehr wird hierdurch auch eine hohe Qualität dieses ergänzenden Instruments sichergestellt; schließlich sehen sich auch die unabhängigen Aufsichtsstellen im Falle unzureichender Pflichterfüllung erheblichen Bußgeldern ausgesetzt.

4.6.1.2.2 Konkrete Auswirkungen

Es stellt sich daher die Frage, inwieweit die Anforderungen an Verhaltensregeln bezüglich der Umsetzungsakte im jeweiligen Drittland über das hinausgehen müssen, was zum Beispiel durch Standarddatenschutzklauseln oder Binding Corporate Rules gewährleistet wird. Weder Standarddatenschutzklauseln noch BCR werden etwaige Widersprüche zum nationalen Recht des Drittlandes auflösen können noch ggf. bestehende (gesetzliche) Rechtsbehelfe schaffen können. Binding Corporate Rules und Standarddatenschutzklauseln sind dabei zwar von den Aufsichtsbehörden abgesegnete Verträge, sie bleiben aber eben auch bilaterale Verträge, die im Weiteren keine weitergehenden, dem jeweiligen Rechtfertigungstatbestand inhärenten unabhängigen Überprüfungsmechanismen beinhalten. Vielmehr obliegt es ausschließlich der staatlichen Aufsicht die Einhaltung dieser Vorgaben zu kontrollieren.

Versteht man BCR sodann als eine besondere Form der Verhaltensregeln, so ergibt sich ein relatives klares Bild, wo die konkreten Potentiale der Rechtfertigung des Drittstaatentransfers durch Verhaltensregeln liegen. Aufsetzend auf den Anforderungen der BCR sowie Standarddatenschutzklauseln werden an den Inhalt der Verhaltensregeln keine besonderen Anforderungen gestellt werden können. Vielmehr könnte argumentiert werden, dass sogar geringere Anforde-

rungen ausreichen müssten, da dieses »Minus« durch die weiteren Sicherungsmechanismen der Verhaltensregeln kompensiert würde.

4.6.1.3 Vorteile/Chancen

Verhaltensregeln bieten Verantwortlichen wie Auftragsverarbeitern in Branchen, in denen ein Datentransfer auch außerhalb der eigenen Unternehmensgruppe erforderlich ist, die Möglichkeit anstelle individueller Verhandlungen mit den Aufsichtsbehörden zu zentralisieren.

Verhaltensregeln können zudem als Maßstab realistischer (Mindest-)Standards in jeweiligen Branchen dienen und somit die europaweite Auslegung der DS-GVO frühzeitig und sachdienlich beeinflussen. Es ist daher nicht auszuschließen, dass staatliche Aufsichtsstellen das in Verhaltensregeln niedergelegte (Mindest-)Niveau bei allen Prüfungen als Referenz heranziehen.

Verhaltensregeln können zudem durch die EU-Kommission für allgemeingültig erklärt werden. Bislang gibt es noch keine solchen Verhaltensregeln, die sich der Rechtfertigung von Datentransfers widmen.

4.6.2 Zertifizierung

Nach Art. 46 Abs. 2 lit. f DS-GVO und Art. 42 Abs. 2 DS-GVO kann auch ein genehmigter Zertifizierungsmechanismus als geeignete Garantie dienen, wenn er zusammen geht mit rechtlich durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland, diese Garantien auch anzuwenden und die Betroffenenrechte einzuhalten. Es gelten grundsätzlich die gleichen Rahmenbedingungen wie auch für die genehmigten Verhaltensregeln.

Information

Stufe: Prüfung der zulässigen Erhebung der Daten beim EU-Unternehmen.

Stufe: Prüfung des Vorliegens der Voraussetzungen der Privacy Shield Zertifizierung.

4.7 USA: Privacy Shield

Die EU-Kommission hat am 12. Juli 2016 den »EU-US Datenschutzschild« (engl. »Privacy Shield«) förmlich angenommen. Der Umsetzungsbeschluss trat mit Zuleitung an die EU-Mitgliedstaaten unverzüglich in Kraft. Damit wurde nach dem Aus für »Safe-Harbor« ein neuer Rahmen für den kommerziellen Austausch von personenbezogenen Daten zwischen der Europäischen Union und den Vereinigten Staaten erzielt. Das Privacy Shield ist eine »Angemessenheitsentscheidung« (C (2016) 4176 final) der EU-Kommission gem. Art. 25 Abs. 6 RL 95/46 EG bzw. Art. 45 DS-GVO. Damit wurde von der EU-Kommission festgestellt, dass die USA ein angemessenes Datenschutzniveau gewährleistet und personenbezogene Daten aus den Mitgliedstaaten der EU ohne (weitere) Genehmigung[7] in die USA fließen können. Voraussetzung hierfür ist, dass die an dem Datenaustausch beteiligten US-Unternehmen bestimmte informatorische und formale Auflagen erfüllen, sowie die Datenschutzgrundsätze nach Anhang II des Privacy-Shield-Beschlusses

7 Siehe Art. 45 Abs. 1 S. 2 DS-GVO.

einhalten. Der Abschluss von Standardvertragsklauseln ist für zertifizierte Unternehmen nicht mehr erforderlich.

Beachte!

Zusätzlicher Auftragsverarbeitungsvertrag trotz Privacy Shield Zertifizierung: Werden personenbezogene Daten im Auftrag aus der EU in die USA übermittelt, so muss unabhängig davon, ob das US-Unternehmen privacy-zertifiziert ist, ein (Auftragsverarbeitungs-) Vertrag zwischen den Parteien geschlossen werden (siehe Anhang II Zusatzgrundsätze III Nr. 10 »Obligatorische Verträge bei Weitergabe«). Für die (noch) auf das BDSG fokussierten Leser fühlt sich diese Anforderung möglicherweise falsch an, da nach dem BDSG aufgrund § 3 Nr. 8 BDSG eine ADV mit einem Unternehmen in einem Drittland nicht möglich war. Betrachtet man jedoch die RL 95/46 EG und vor allem die DS-GVO so fügt sich diese Anforderung logisch ein. Aufgrund der Erweiterung des räumlichen Geltungsbereichs in Art. 3 DS-GVO auf außerhalb der Europäischen Union ist zukünftig auch eine Auftragsverarbeitung außerhalb der EU möglich. Für die Auftragsverarbeitung in den USA haben die Verfasser des Privacy Shield Beschlusses explizit festgeschrieben, dass in diesem Fall ein Auftragsverarbeitungsvertrag geschlossen werden muss, der folgende Punkte enthält:

- Auftragsverarbeiter handelt nur auf Weisung des Verantwortlichen,
- Auftragsverarbeiter stellt geeignete technische und organisatorische Maßnahmen sicher,
- Auftragsverarbeiter unterstützt den Verantwortlichen hinsichtlich der Betroffenenrechte (von Bedeutung aufgrund Art. 13 Abs. 1 lit. f DS-GVO).

Die Entscheidung dem Privacy Shield beizutreten ist vollkommen freiwillig – die wirksame Einhaltung der Grundsätze ist obligatorisch.

Seit dem 1.8.2016 können US-Unternehmen dem Privacy Shield beitreten. Aktuell sind 2468 Unternehmen registriert (Stand 1.9.2017). Die Liste ist öffentlich zugänglich ↗Webseite (https://www.privacyshield.gov/list). Das amerikanische Handelsministerium (FTC) vergibt die Zertifikate, nachdem das Unternehmen für den Zertifizierungsprozess alle erforderlichen Angaben gemacht hat (Self-Certify). Die Zertifizierung ist jährlich zu erneuern (siehe Anhang II Überblick I Nr. 3). Für den Fall, dass das Unternehmen die Zertifizierung nicht nach einem Jahr erneuert, streicht die FTC das Unternehmen von der Liste. Das Unternehmen wird dann in der Privacy Shield Liste als »inactiv« geführt (Am 1.9.2017 waren 11 Unternehmen als »inactive« gelistet).

Die Regelungsinhalte des Privacy Shield ergeben sich aus Anhang II des Privacy Beschlusses. Unter (I) wird im »Überblick« die Motivation für den gemeinsamen Datenaustausch beschrieben, ebenso die allgemeinen Pflichten. Unter (II) werden »Grundsätze« festgeschrieben, die dem Schutz der Betroffenen dienen. Hierzu zählen u. a. die Information über

die Teilnahme am Privacy Shield, die Möglichkeit, der Datenweitergabe zu widersprechen (opt-out), Auskunftsrecht und Rechtsschutzmöglichkeiten. Unter (III) werden »Zusatzgrundsätze« beschrieben, die Unternehmensprozesse betreffen, wie z. B. Ausnahmen für den journalistischen Bereich, Due-Diligence und Wirtschaftsprüfung, Rolle der Datenschutzbehörde, Audits und Beschwerdeverfahren.

Aufgrund einer sogenannten Executive Order von Präsident Trump vom 25.1.2017 wurden Stimmen laut, die das Fortbestehen des Privacy Shields in Frage stellten. In einer Antwort der EU-Kommissarin Jourová vom 5.4.2017 auf eine parlamentarische Frage des Europäischen Parlaments wird mitgeteilt, dass die US-Justizbehörde in einem Antwortschreiben offiziel bestätigt, dass Section 14 der Executive Order die Verpflichtungen aus dem Privacy Shield nicht tangiert. Damit wird bis auf weiteres das Privacy Shield als Grundlage für den transatlantischen Datenaustausch dienen.

Darüber hinaus ist darauf hinzuweisen, dass die französische Verbraucherschutzorganisation La Quadrature du Net (Case T-738/16) sowie die irische NGO Digital Rights Ireland (Case T-738/16) in einem getrennten Verfahren auf EU-Ebene gegen das Privacy Shield der EU-Kommission geklagt haben. Bevor der EuGH sich mit dem Privacy Shield in diesen Verfahren auseinandersetzt, muss erst geklärt werden, ob die beiden Parteien als Nichtregierungsorganisationen unter EU-Recht klagebefugt sind. Diese Entscheidung steht derzeit noch aus.

Unabhängig davon werden die Vereinigten Staaten und die Europäische Union im September 2017 das erste Review des Privacy Shields gemeinsam durchführen (siehe ↗http://europa.eu/rapid/press-release_SPEECH-17-826_en.htm?locale=en).

Weitere Informationen hierzu finden Sie:

↗Pressemitteilung
↗Angemessenheitsbeschluss ((EU)2016/1250 der Kommission vom 12. Juli 2016)
↗Anhänge/Annex
↗FAQ
↗Factsheet
↗Mitteilung Frau Jourová zur Executive Order

Die EU-Kommission hat für EU-Bürger einen ↗Leitfaden zur Erläuterung der Rechtsbehelfe bei Datenschutzverstößen veröffentlicht.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen hat ↗Fragen und Antworten zum Privacy Shield veröffentlicht.

Auch das Bayerische Landesamt für Datenschutzaufsicht hat einen Überblick zum Privacy Shield und ein Beschwerdeformular für Bürger ↗veröffentlicht.

5 Konzerninterne Datenübermittlung

5 Konzerninterne Datenübermittlung

5.1 Allgemeines

Anders als beispielsweise im Steuer- und Gesellschaftsrecht gab und gibt es im Datenschutzrecht kein Konzernprivileg. Die Zulässigkeit von Verarbeitungen personenbezogener Daten ist von jeder einzelnen Konzerngesellschaft individuell nach den allgemeinen Regeln der DS-GVO – deren Anwendbarkeit vorausgesetzt – zu prüfen.

Wenn nachfolgend dennoch auf einige Aspekte bei der Verarbeitung von Beschäftigten- und Kundendaten eingegangen wird, dann deshalb, weil diesbezüglich teilweise Rechtsunsicherheit besteht bzw. sie von der bisherigen Praxis abweichen können. Dabei macht es keinen Unterschied, ob die Verarbeitungen konzernintern oder -extern bzw. national oder international erfolgen.

5.2 Grundsätze für die Verarbeitung von personenbezogenen Daten

Die Grundsätze für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO aufgeführt. Hierzu gehört der Transparenzgrundsatz, wonach die Verarbeitung für die betroffene Person in einer nachvollziehbaren Weise zu erfolgen hat. Für Datenverarbeitungen im Beschäftigungskontext können die Mitgliedstaaten gemäß Art. 88 DS-GVO »spezifischere« Regelungen erlassen. Ob und wie Deutschland von dieser nationalen Öffnungsklausel etwa durch ein immer wieder in die Diskussion gebrachtes Beschäftigtendatenschutzgesetz Gebrauch macht, bleibt abzuwarten. Bis dato gibt es nur eine knappe Aussage zu Transparenzanforderungen in § 26 Abs. 4 BDSG (2018). Auf sie wird im Kontext von Betriebsvereinbarungen (unter 5.3.4) eingegangen.

5.3 Rechtmäßigkeit der Verarbeitung

Eine Verarbeitung personenbezogener Daten von Beschäftigten und Kunden darf nur dann durchgeführt werden, wenn sie durch einen der in Art. 6 Abs. 1 DS-GVO abschließend aufgeführten Erlaubnistatbestände legitimiert ist. Dabei ergeben sich bei den nachfolgenden drei Erlaubnistatbeständen gewisse Besonderheiten.

5.3.1 Einwilligung

Eine Datenverarbeitung ist rechtmäßig, wenn die betroffene Person wirksam in sie eingewilligt hat. Eine Einwilligung ist gemäß Art. 4 Abs. 11 DS-GVO jede freiwillig für den konkreten Fall, auf informierter Basis unmissverständlich abgegebene Willenserklärung bzw. bestätigende Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden Daten einverstanden ist. An der erforderlichen Freiwilligkeit kann es mangeln, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, ErwG. 43 DS-GVO. Der Vorschlag der EU-Kommission für die DS-GVO enthielt noch die

Aussage, dass solch ein Ungleichgewicht im Beschäftigungsverhältnis besteht. Durch die Streichung dieser Festlegung ist klargestellt, dass Einwilligungen grundsätzlich auch im Beschäftigungsverhältnis möglich sind.[8]

Wann die Einwilligung eines Beschäftigten freiwillig und damit wirksam ist, gehört zu den Regelungsfragen, die gemäß Art. 88 DS-GVO durch die Mitgliedstaaten »spezifischer« geregelt werden können, ErwG. 155 DS-GVO. Deutschland hat von dieser nationalen Öffnungsklausel mit der Verabschiedung des DSAnpUG-EU Gebrauch gemacht und in § 26 Abs. 2 BDSG (2018) Kriterien festgelegt, die bei der Bestimmung der Freiwilligkeit der Einwilligung zu berücksichtigen sind. Die individuell bestehende Abhängigkeit und die Umstände, unter denen die Einwilligung erfolgt, sind demnach Kriterien, die zu würdigen sind. Als Indizien, die für die Freiwilligkeit der Einwilligung sprechen, nennt § 26 Abs. 2 S. 2 BDSG (2018) die rechtliche oder wirtschaftliche Vorteilhaftigkeit für den Beschäftigen. Ob und in welchem Umfang angesichts der Ausgestaltung der Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis durch den nationalen Gesetzgeber ergänzend bei deren Interpretation auf die »Opinon on data processing at work« der europäischen Aufsichtsbehörden zurückgegriffen werden kann, ist fraglich. Zum einen hat der nationale Gesetzgeber klare Kriterien benannt, die wenig Interpretationsspielraum zulassen und zum anderen ist die Meinung der europäischen Aufsichtsbehörden gegenüber der neuen Gesetzeslange in Deutschland deutlich restriktiver, was daran liegt, dass sie immer auch die jeweiligen nationalen arbeitsrechtlichen Gegebenheiten berücksichtigen müssen.

Gemäß § 26 Abs. 2 S. 3 BDSG (2018) bedarf die Einwilligung der Schriftform. Ob es sich dabei um eine zulässige Konkretisierung der Nachweispflicht des Arbeitgebers handelt (so die Gesetzesbegründung) oder um eine unzulässige Überschreitung des durch Art. 88 DS-GVO gesetzten Rahmens, werden im Zweifel die Gerichte zu klären haben. So oder so muss der Arbeitgeber nachweisen können, dass er den Beschäftigten vollumfänglich, und zwar in Textform (§ 26 Abs. 2 S. 4 BDSG (2018)) informiert hat und eine auf die konkrete Verarbeitung bezogene Einwilligung erhalten hat.

5.3.2 Vertragserfüllung

Verarbeitungen personenbezogener Daten von Beschäftigen einer Konzerngesellschaft lassen sich über Art. 6 Abs. 1 lit. b DS-GVO legitimieren. Mit § 26 Abs. 1 BDSG (2018) hat der deutsche Gesetzgeber eine spezifischere Vorschrift im Sinne von Art. 88 Abs. 1 DS-GVO geschaffen. Demnach dürfen personenbezogenen Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Der deutsche Gesetzgeber hat mit der Aufspaltung des Begriffs des Beschäftigungsverhältnisses lediglich beispielhaft zu verstehen gegeben, was hierunter auf jeden Fall zu verstehen ist, wobei er auf die bekannte Terminologie von § 32 BDSG (2009) zurückgegriffen hat. Dies bedeutet allerdings nicht, dass andere Verarbeitungen

8 So auch die Art. 29-Datenschutzgruppe in »Opinion 2/2017 on data processing at work« (WP 249).

von personenbezogenen Daten von Beschäftigten, die zur Erfüllung des Beschäftigungsverhältnisses erforderlich sind, nicht zulässig wären. Eine solche Einschränkung eines Erlaubnistatbestands wäre europarechtswidrig.[9] Dankenswerterweise hat der deutsche Gesetzgeber in § 26 Abs. 8 BDSG (2018) klargestellt, dass der datenschutzrechtliche Begriff des Beschäftigten umfassend zu verstehen ist.

5.3.3 Wahrnehmung berechtigter Interessen

Die Verarbeitung personenbezogener Daten wird in der Praxis oft durch die Berufung auf die Wahrnehmung berechtigter Interessen legitimiert. Was berechtigte Interessen im Sinne von Art. 6 Abs. 1 lit. f DS-GVO sind und wann sie die Interessen oder Rechte der betroffenen Person überwiegen können, haben die europäischen Aufsichtsbehörden ausführlich in ihrer »Stellungnahme zu dem Begriff der berechtigen Interessen des für die Verarbeitung Verantwortlichen« (WP217) ausgeführt.

Der Erlaubnistatbestand der Wahrnehmung berechtigter Interessen ist bei Datenverarbeitungen im Kontext eines Beschäftigungsverhältnisses unzweifelhaft anwendbar. Dies ergibt sich eindeutig aus ErwG. 48.[10] Dessen Satz 1 besagt, dass sich Übermittlungen von Beschäftigten- und Kundendaten an andere Konzerngesellschaften für interne Verwaltungszwecke über diesen Erlaubnistatbestand legitimieren lassen.

Einige sehen hierin ein »kleines Konzernprivileg«. Dies ist unzutreffend, da es hier nicht um eine Besserstellung oder Privilegierung von konzerninternen Übermittlungen gegenüber anderen Verarbeitungen geht. ErwG. 48 regelt nichts Neuartiges, sondern führt lediglich beispielhaft auf, dass für die aufgeführten Konstellationen Übermittlungen bei Vorliegen berechtigter Interessen legitimiert werden können. Den Erlaubnistatbestand der Wahrnehmung berechtigter Interessen hat der europäische Gesetzgeber von der RL 95/46 EG übernommen. Im Gegensatz zu vielen anderen Mitgliedstaaten hat der deutsche Gesetzgeber bei der Umsetzung der RL 95/46 EG allerdings weder die Systematik noch den Wortlaut von Art. 7 RL 95/46 EG eins zu eins übernommen, sondern lediglich einige wenige Anpassungen an dem BDSG (1990) vorgenommen, die den Kern der europäischen Vorgaben nicht voll erfasst haben. Dies erklärt, warum in anderen Mitgliedstaaten die Legitimierung konzerninterner Übermittlungen keine Probleme bereitete und der europäische Gesetzgeber keinen Bedarf für die Aufnahme einer Regelung im Sinne eines wie auch immer formulierten Konzernprivilegs sah. Logischerweise waren auch sämtliche gut gemeinten diesbezüglichen Vorschläge des Europäischen Parlaments zum Scheitern verurteilt. Allerdings sah sich der europäische Gesetzgeber veranlasst, eine Klarstellung in einem Erwägungsgrund vorzunehmen, um die harmonisierte Anwendung des Erlaubnistatbestands der Wahrnehmung berechtigter Interessen zu gewährleisten.

9 EuGH, Urteil vom 24.11.2011, ASNEF und FECEMD, C-468/10 und C-469/10.

10 Auch nach Auffassung der in der Datenschutzgruppe zusammengeschlossenen europäischen Aufsichtsbehörden kann dieser Erlaubnistatbestand im Kontext eines Beschäftigungsverhältnisses angewendet werden, siehe z.B. WP 217 und WP 247.

Als weiteres Beispiel dafür, welche konzerninternen Übermittlungen sich über die Wahrnehmung berechtigter Interessen rechtfertigten lassen können, sehen die europäischen Datenschutzbehörden den Aufbau einer unternehmensweiten internen Mitarbeiterdatenbank mit Kontaktdaten an, WP 217, S. 22.

5.3.4 Betriebsvereinbarung

Praxistipp!

Der Verantwortliche sollte im Falle der Berufung auf den Erlaubnistatbestand der Wahrnehmung berechtigter Interessen diese auf den konkreten Anwendungsfall bezogen dokumentieren. Anderenfalls kann er weder seiner Pflicht zur Rechenschaftslegung aus Art. 5 Abs. 2 DS-GVO noch seiner Pflicht zur Information betroffener Personen (Art. 13 Abs. 1 lit. d, Art. 14 Abs. 2 lit. b und Art. 21 Abs. 1 DS-GVO) adäquat nachkommen.

Die DS-GVO hat in ErwG. 155 klargestellt, dass »spezifischere« Vorschriften für die Verarbeitung von personenbezogenen Daten im Beschäftigtenkontext gemäß Art. 88 DS-GVO in Kollektiv- und Betriebsvereinbarungen getroffen werden können. Diese stellen jedoch keine eigenständigen Erlaubnistatbestände dar, sondern dienen lediglich dazu, eine durch Art. 6 Abs. 1 legitimierte Verarbeitung personenbezogener Daten von Beschäftigten »spezifisch« auf das einzelne Unternehmen bezogen individuell auszugestalten. Der Gesetzgeber setzt damit die Feststellungen des Europäischen Gerichtshofs[11] zur Ausgestaltungsmöglichkeit der Erlaubnistatbestände aus Art. 6 Abs. 1 DS-GVO um, wonach die Mitgliedstaaten diese weder ausweitend oder einschränkend verändern dürfen.

In § 26 Abs. 4 S. 1 BDSG (2018) wiederholt der deutsche Gesetzgeber die Feststellung der DS-GVO, nach der in Kollektivvereinbarungen Sachverhalte des Beschäftigungsverhältnisses datenschutzkonform ausgestaltet werden können. Hierrunter fallen laut Gesetzesbegründung auch Betriebs- und Dienstvereinbarungen. Der zweite Satz dieses Absatzes verweist auf Art. 88 Abs. 2 DS-GVO, wonach bei solchen Vereinbarungen »insbesondere auf die Transparenz der Verarbeitung« zu achten ist. Dies ist zunächst dahingehend zu verstehen, dass Kollektiv- und Betriebsvereinbarungen für Beschäftigte leicht zugänglich sein müssen. Falls der Text einer Betriebsvereinbarung so formuliert ist, dass ein durchschnittlicher Beschäftigter nicht unzweifelhaft erkennen kann für welche Zwecke seine personenbezogene Daten verarbeitet werden sollen, ist zusätzlich eine allgemeinverständliche Zusammenfassung beizufügen. Andernfalls wird der gesetzlichen Pflicht zur Verwendung »einer klaren und einfachen Sprache« (so Art. 12 DS-GVO) nicht entsprochen.

11 EuGH, Urteil vom 24.11.2011 (ASNEF) und (FECEMD), C-468/10 und C-469/10.

5.4 Auftragsverarbeitung durch Konzerngesellschaften

Die Grundsätze für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO aufgeführt. Hierzu gehört der Transparenzgrundsatz, wonach die Verarbeitung für die betroffene Person in einer nachvollziehbaren Weise zu erfolgen hat. Für Datenverarbeitungen im Beschäftigungskontext können die Mitgliedstaaten gemäß Art. 88 DS-GVO »spezifischere« Regelungen erlassen. Ob und wie Deutschland von dieser nationalen Öffnungsklausel etwa durch ein immer wieder in die Diskussion gebrachtes Beschäftigtendatenschutzgesetz Gebrauch macht, bleibt abzuwarten. Bis dato gibt es nur eine knappe Aussage zu Transparenzanforderungen in § 26 Abs. 4 BDSG (2018). Auf sie wird im Kontext von Betriebsvereinbarungen (unter 6.3.4) eingegangen.

Aufgrund der allgemeinen Tendenz Abläufe zu zentralisieren kommt es immer häufiger vor, dass einzelne Konzerngesellschaften für andere Konzerngesellschaften Dienstleistung übernehmen, wie beispielsweise das Accounting, Payroll, Recruiting etc.

5.4.1 Vertrag zur Auftragsverarbeitung

Soweit dabei personenbezogene Daten im Auftrag verarbeitet werden, haben die Konzerngesellschaften auch für diese konzerninternen Übermittlungen einen Vertrag für die Auftragsverarbeitung gemäß Art. 28 DS-GVO zu schließen.

Praxistipp!

Um zu vermeiden, dass alle beauftragenden Konzerngesellschaften mit der einen beauftragten Gesellschaft individuelle Verträge gemäß Art. 28 DS-GVO schließen, kann man auch folgende Lösung wählen: Die Konzernmutter (Verantwortlicher im Sinne des Art. 4 Abs. 7) schließt mit der beauftragten Konzerngesellschaft (Auftragsverarbeiter im Sinne des Art. 4 Abs. 8 DS-GVO) einen Vertrag gemäß Art. 28 DS-GVO, dem die anderen Konzerngesellschaften (als Verantwortliche) beitreten. Der Beitritt muss dokumentiert, das heißt nachweisbar sein, damit die Konzerngesellschaften ihre Rechenschaftspflicht erfüllen.

5.4.2 Schriftlichkeit

Der Vertrag über die Auftragsverarbeitung muss »schriftlich« erfolgen. Dies bedeutet nach dem europäischen Verständnis jedoch nicht, dass es für die Wirksamkeit des Vertrages der eigenhändigen Unterschrift der Vertragsparteien bedarf. Schriftlich in Art. 28 Abs. 9 DS-GVO ist im Sinne von »dokumentiert«[12] zu verstehen, wofür ein elektronisches Format ausreichend ist. Die teilweise gegenteilige in Deutschland vertretene Auffassung, wonach schriftlich im Sinne des § 126

12 So auch schon Art. 17 Abs. 4 RL 95/46 EG.

BGB als zwingendes Schriftformerfordernis zu verstehen ist, lässt sich somit nicht weiter aufrechterhalten. Allerdings ist zu bedenken, dass Konzerngesellschaften ihrer Rechenschaftspflicht natürlich genügen müssen. Dieser Verpflichtung können sie auch dadurch entsprechen, dass sie den Vertrag zur Auftragsverarbeitung als Anlage zu dem Leistungsvertrag unterschreiben, was bei der Einbeziehung von konzernexternen Partnern sowieso empfehlenswert ist.

5.4.3 Legitimierung ohne »Privileg der Auftragsverarbeitung«

Das deutsche Datenschutzrecht hat bei der Auftragsdatenverarbeitung (so die übliche Bezeichnung in Deutschland) bisher wie folgt differenziert:[13] Erfolgt die Verarbeitung der Daten im Auftrag durch einen Dienstleister (Auftragsdatenverarbeiter) innerhalb des Europäischen Wirtschaftsraums (EWR), ist der Datentransfer zu ihm eine legitimierungsfreie Weitergabe. Demgegenüber ist bei der Ausübung der gleichen Tätigkeit der Dienstleister außerhalb des EWR ein Dritter und der Datentransfer bedarf einer Legitimierung, welche man mehrheitlich in der »Wahrnehmung berechtigter Interessen« im Sinne des § 28 Abs. 1 Nr. 2 BDSG (2001) sieht.[14]

Diese Differenzierung kennt weder das europäische Datenschutzrecht der RL 95/46 EG noch das der DS-GVO. Der Dienstleister, der im Auftrag eines Verantwortlichen personenbezogene Daten verarbeitet, ist unabhängig vom Ort der Verarbeitung stets ein Auftragsverarbeiter (Art. 4 Abs. 8 DS-GVO). Der Datentransfer zu ihm ist immer eine Übermittlung und damit eine Verarbeitung im Sinne des europäischen Rechts (Art. 4 Abs. 2 DS-GVO). Die erforderliche Legitimierung für die Übermittlung an den Auftragsverarbeiter, aber auch allen anderen Verarbeitungen in diesem Zusammenhang, lassen sich aus der Rolle des Verantwortlichen und seiner ihm kraft Gesetzes zugeschriebenen Rolle ableiten. Es bedarf mithin keines weiteren oder speziellen Erlaubnistatbestands. Das charakterisierende Kriterium des Verantwortlichen ist seine Entscheidungsbefugnis, die Zwecke und Mittel der Verarbeitung bestimmen zu können. Wenn ein Verantwortlicher eine Verarbeitung auf der Basis eines der in Art. 6 Abs. 1 DS-GVO aufgeführten Erlaubnistatbestände durchführen darf, kann er auch frei darüber entscheiden, ob er die Verarbeitung – ganz oder teilweise – selbst durchführt oder hiermit einen Auftragsverarbeiter beauftragt und ihm ggfs. personenbezogene Daten übermittelt.

5.5 Gemeinsam für die Verarbeitung Verantwortliche

Nach der DS-GVO können mehrere Verantwortliche die Zwecke und Mittel der Verarbeitung gemeinsam festlegen, Art. 4 Abs. 7 DS-GVO. In solch einem Fall haben die betreffenden Konzerngesellschaften eine transparente Vereinbarung zu schließen, die den Anforderungen von Art. 26 DS-GVO genügt. Ist eine Konzerngesellschaft der gemeinsam für die Verarbeitung Verantwortlichen in einem unsicheren Drittland niedergelassen, bedarf es zusätzlich »geeigneter Garantien«, z. B. in Form von BCR.

13 Spätestens ab dem 25. Mai 2018 ist diese Rechtsauffassung nicht mehr vertretbar.

14 Ausführlich hierzu Drewes/Monreal in PinG 2014, S. 143ff.

6 Begriffsbestimmungen, Materialien, Grafiken und Übersichten

6 Begriffsbestimmungen, Materialien, Grafiken und Übersichten

6.1 Begriffsbestimmungen

Im Folgenden werden einige zentrale Begriffe des Datenschutzes kurz erläutert:

- **Auftragsverarbeitung/Auftragsverarbeiter**
  Eine Datenverarbeitung im Auftrag ist eine Datenverarbeitung personenbezogener Daten durch den Auftragsverarbeiter (Auftragnehmer) nach Weisung und im Auftrag des Verantwortlichen (Auftraggeber). Auftragsverarbeiter ist eine natürliche oder juristische Person, die Daten im Auftrag des Verantwortlichen verarbeitet, vgl. Art. 4 Nr. 8 DS-GVO. Aufgrund der direkten Anwendung der DS-GVO wird keine Unterscheidung mehr getroffen zwischen einer Auftragsverarbeitung in der EU oder in einem Staat außerhalb (Drittland). Eine Beschränkung der Privilegierung der Auftragsverarbeitung ergab sich bisher aus §3 Abs. 8 S. 2 BDSG.

- **Besondere Arten personenbezogener Daten**
  Von den allgemeinen personenbezogenen Daten sind die besonderen Kategorien von Daten zu unterscheiden. Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit sowie die Verarbeitung von genetischen Daten, biometrischen Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person, vgl. Art. 9 DS-GVO.

- **Betroffene Person**
  Jede natürliche Person, um deren personenbezogene Daten es geht und die davor zu schützen ist, dass sie durch die Verarbeitung in ihrem Recht auf Schutz personenbezogener Daten beeinträchtigt wird, vgl. Klammerzusatz in Definition von Art. 4 Nr. 1 DS-GVO.

- **Datenexporteur**
  Datenexporteur ist der für die Verarbeitung Verantwortliche, der personenbezogene Daten übermittelt.

- **Datenimporteur**
  Datenimporteur ist der für die Verarbeitung Verantwortliche, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten für die Verarbeitung entgegenzunehmen.

- **Dritter**
  Der Ausdruck »Dritter« bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (Art. 4 Nr. 10 DS-GVO). Nicht unter den Begriff »Dritter« fallen rechtlich unselbstständige Zweigstellen eines Unternehmens (wie z. B. Filialen). Rechtlich selbstständige Einrichtungen – wie Betriebskrankenkassen – sind jedoch auch dann Dritte, wenn sie organisatorisch, räumlich oder personell mit der speichernden Stelle verbunden sind.

- **Drittland**
  Als Drittländer werden alle anderen Staaten außerhalb der EU bezeichnet (zu EWR siehe 2.1).

- **Einwilligung**
  Jede von der betroffenen Person freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung, in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, ist eine »Einwilligung«, vgl. Art. 4 Nr. 11 DS-GVO.

- **Empfänger**
  Empfänger ist jede Stelle, die Daten erhält.

- **Personenbezogene Daten**
  Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (die auch als die »betroffene Person« bezeichnet wird); Juristische Personen des privaten Rechts (z. B. AG, GmbH) werden damit nicht erfasst. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung (z. B. Name), zu einer Kennnummer (z. B. Sozialversicherungsnummer, Steueridentifikationsnummer), zu Standortdaten, zu einer Online-Kennung (z. B. IP-Adresse oder Cookie-Kennung) oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann, vgl. Art. 4 Nr. 1 DS-GVO.

- **Unternehmen**
  Eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig wirtschaftlichen Tätigkeiten nachgehen, vgl. Art. 4 Nr. 18 DS-GVO. Damit ist der datenschutzrechtliche Unternehmensbegriff sehr weit und umfasst jedes Unternehmen unabhängig von Größe und Branche, so dass z. B. auch Freiberufler erfasst sind.

- **Unternehmensgruppe**
  Eine Gruppe, die aus einem herrschenden Unternehmen und den von diesen abhängigen Unternehmen besteht; vgl. Art. 4 Nr. 19 DS-GVO sowie Art. 37, 47 und 88 DS-GVO, wo die Definition eine Rolle spielt. Die Definition ist auf einen Unternehmensverbund beschränkt, wo ein Unternehmen einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann z. B. aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen (ErwG. 37). Davon abzugrenzen sind andere Begriffsbestimmungen wie z. B. eine Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, die aufgrund der Selbständigkeit nicht vom Begriff erfasst sind.

- **Verarbeitung personenbezogener Daten**
  Verarbeitung ist jeder Vorgang, mit oder ohne Hilfe automatisierter Verfahren, im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung, vgl. Art. 4 Nr. 2 DS-GVO.

- **Verbindliche interne Datenschutzvorschriften**
  Verbindliche interne Datenschutzvorschriften (engl. Binding Corporate Rules; BCRs) sind Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats der Union niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter ders. Unternehmensgruppe oder ders. Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern, vgl. Art. 4 Nr. 20 DS-GVO.

- **Verantwortlicher**
  Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, vgl. Art. 4 Nr. 7 DS-GVO.

- **Vertreter**
  Eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt, vgl. Art. 4 Nr. 17. Diese Definition ist nur für nicht in der Union niedergelassene Verantwortliche oder Auftragsverarbeiter relevant.

6.2 Materialien zum EU-US Privacy Shield

6.2.1 Die Privacy Shield Principles

Informationspflicht

Die Organisation muss Privatpersonen über Folgendes informieren:

- ihre Teilnahme am Datenschutzschild mit einem Link zur Datenschutzschild-Liste oder der Webanschrift der Liste,

- die Arten der erfassten personenbezogenen Daten und gegebenenfalls die Einrichtungen oder Tochterunternehmen der Organisation, die die Grundsätze ebenfalls einhalten,
- ihre Verpflichtung, die Grundsätze auf alle aus der EU empfangenen personenbezogenen Daten unter Zugrundelegung des Datenschutzschilds anzuwenden,
- zu welchem Zweck sie die personenbezogenen Daten über sie erhebt und verwendet,
- wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, wozu auch Angaben zu einer relevanten Einrichtung in der EU gehören, die auf derartige Nachfragen oder Beschwerden eingehen kann,
- die Kategorie und Identität von Dritten, an die die Daten weitergegeben werden, sowie der Zweck der Weitergabe,
- das Recht von Privatpersonen auf Zugang zu ihren personenbezogenen Daten,
- welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe ihrer personenbezogenen Daten einzuschränken,
- das zur Bearbeitung von Beschwerden und für einen kostenlosen Rechtsschutz für die Privatperson benannte unabhängige Streitbeilegungsgremium, und ob es sich 1) um das von Datenschutzbehörden eingerichtete Gremium, 2) um einen in der EU ansässigen Anbieter für alternative Streitbeilegung oder 3) um einen in den Vereinigten Staaten ansässigen Anbieter für alternative Streitbeilegung handelt,
- die für die Organisation geltenden Ermittlungs- und Durchsetzungsbefugnisse der FTC, des Verkehrsministeriums oder einer anderen bevollmächtigten US-Behörde,
- die Möglichkeit, unter bestimmten Bedingungen ein verbindliches Schiedsverfahren anzustrengen,
- die Bestimmung, personenbezogene Daten auf rechtmäßige Anfrage von Behörden offenzulegen, um Erfordernissen der nationalen Sicherheit oder der Strafverfolgung nachzukommen, und
- die Haftung der Organisation bei Weitergabe an Dritte.

Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig ersucht werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

Wahlmöglichkeit

Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen (»Opt-out«), ob ihre personenbezogenen Daten i) an Dritte weitergegeben werden sollen oder ii) für einen Zweck verwendet werden sollen, der sich von dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck wesentlich unterscheidet. Der betroffenen Person muss die Ausübung ihres Wahlrechts durch leicht erkennbare, verständliche und leicht zugängliche Verfahren ermöglicht werden.

Abweichend vom vorstehenden Absatz unterliegt die Übermittlung solcher Daten an einen Dritten nicht dem Grundsatz der Wahlmöglichkeit, wenn dieser im Auftrag oder auf Anweisung der Organisation tätig ist. Die Organisation schließt jedoch stets einen Vertrag mit dem Beauftragten.

Bei sensiblen Daten (d. h. Angaben über den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder weltanschauliche Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben) benötigen die Organisationen die ausdrückliche Zustimmung (»Opt-in«) der betroffenen Personen, wenn diese Daten

I. an Dritte weitergegeben oder
II. für einen anderen als den ursprünglichen Erhebungszweck oder den Zweck verwendet werden sollen, dem die betroffene Person nachträglich durch Ausübung des Wahlrechts zugestimmt hat. Darüber hinaus sollen die Organisationen alle ihnen von Dritten übermittelten personenbezogenen Daten als sensibel behandeln, die der Übermittler als sensibel einstuft und behandelt.

Verantwortlichkeit für Weitergabe

Eine Organisation darf personenbezogene Daten nur dann an Dritte, die als für die Verarbeitung Verantwortliche tätig sind, weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Die Organisation muss auch einen Vertrag mit dem als für die Verarbeitung Verantwortlichen tätigen Dritten schließen, in dem festgelegt ist, dass diese Daten nur in begrenztem Rahmen für bestimmte Zwecke im Einklang mit der von der betroffenen Person erteilten Zustimmung verarbeitet werden dürfen und dass der Empfänger das gleiche Schutzniveau vorsieht wie die Grundsätze und er die Organisation entsprechend unterrichten muss, wenn er feststellt, dass er diese Verpflichtung nicht mehr erfüllen kann. Der Vertrag muss festlegen, dass im Falle einer derartigen Festlegung der als Verantwortlicher tätige Dritte die Verarbeitung einstellt oder mit anderen sinnvollen und geeigneten Maßnahmen Abhilfe schafft.

Bei der Weitergabe von personenbezogenen Daten an einen Dritten, der in ihrem Auftrag und auf ihre Anweisung tätig ist, gilt für eine Organisation Folgendes:

I. sie darf diese Daten nur in begrenztem Rahmen für bestimmte Zwecke weitergeben;
II. sie muss sich vergewissern, dass der Beauftragte verpflichtet ist, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den Grundsätzen gefordert wird;
III. sie muss mit angemessenen und geeigneten Schritten sicherstellen, dass der Beauftragte die weitergegebenen personenbezogenen Daten in einer den Verpflichtungen der Organisation im Rahmen der Grundsätze konformen Weise verarbeitet;
IV. sie muss vom Beauftragten verlangen, dass er sie unterrichtet, wenn er feststellt, dass er seine Verpflichtung, das gleiche Schutzniveau vorzusehen wie in den Grundsätzen gefordert, nicht mehr erfüllen kann,
V. sie muss auf entsprechenden Hinweis, einschließlich nach
VI. sinnvolle und geeignete Schritte unternehmen, um eine unbefugte Verarbeitung zu unterbinden;
VII. sie muss dem Ministerium auf Verlangen eine Zusammenfassung oder ein Exemplar der einschlägigen Datenschutzbestimmungen

Sicherheit

Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, müssen angemessene und geeignete Maßnahmen ergreifen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen; dabei sind insbesondere die Risiken bei der Verarbeitung und die Art der personenbezogenen Daten zu berücksichtigen.

Datenintegrität und Zweckbindung

In Übereinstimmung mit den Grundsätzen müssen personenbezogene Daten auf die Informationen beschränkt sein, die für den Verarbeitungszweck erheblich sind.2 Eine Organisation darf personenbezogene Daten nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar ist, dem der Betroffene nachträglich zugestimmt hat. In dem für diese Zwecke notwendigen Umfang muss die Organisation durch angemessene Maßnahmen gewährleisten, dass die personenbezogenen Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind. Die Organisation muss die Grundsätze so lange einhalten, wie sie diese Informationen aufbewahrt. Die Daten dürfen nur so lange in einer Form aufbewahrt werden, die eine Person identifiziert oder identifizierbar macht3, wie damit ein Verarbeitungszweck im Sinne von 5a erfüllt wird. Diese Verpflichtung hindert Organisationen nicht daran, personengebundene Informationen über längere Zeiträume zu verarbeiten, solange und soweit diese Verarbeitung hinreichend den Zwecken einer Archivierung im öffentlichen Interesse, des Journalismus, der Literatur und Kunst, der wissenschaftlichen oder historischen Forschung und der statistischen Analyse dient. In diesen Fällen unterliegt die Verarbeitung den anderen Grundsätzen und Bestimmungen der Regelung. Die Organisationen sollen zur Einhaltung dieser Bestimmung angemessene und geeignete Maßnahmen ergreifen.

Auskunftsrecht

Privatpersonen müssen Zugang zu den personenbezogenen Daten haben, die eine Organisation über sie besitzt, und sie müssen die Möglichkeit haben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind oder unter Missachtung der Grundsätze verarbeitet wurden, es sei denn, die Belastung oder die Kosten für die Gewährung des Zugangs würden in dem jeweiligen Fall in einem Missverhältnis zu den Nachteilen für den Betroffenen stehen, oder Rechte anderer Personen als des Betroffenen würden verletzt.

Rechtsschutz, Durchsetzung und Haftung

Für einen effektiven Schutz der Privatsphäre müssen belastbare Mechanismen geschaffen werden, die die Einhaltung der Grundsätze gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt. Diese Mechanismen müssen mindestens Folgendes umfassen:

I. leicht zugängliche, von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden, die betroffene Personen unter Berufung auf die Grundsätze erhoben haben, ohne Kosten für den Betroffenen untersucht und zügig behandelt werden und nach denen Schadenersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen;
II. Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Organisationen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden, und insbesondere in Bezug auf Verstöße;
III. Verpflichtungen zur Lösung von Problemen, die daraus resultieren, dass Organisationen die Einhaltung der Grundsätze zwar erklärt, sich aber trotzdem nicht daran gehalten haben, sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Grundsätze einhalten.

Organisationen und die von ihnen gewählten unabhängigen Beschwerdestellen werden rasch auf Anfragen und Auskunftsbegehren des Ministeriums reagieren, die mit dem Datenschutzschild im Zusammenhang stehen.

Alle Organisationen müssen zügig auf von Behörden der EU-Mitgliedstaaten über das Ministerium weitergeleitete Beschwerden bezüglich der Einhaltung der Grundsätze reagieren. Organisationen, die sich für eine Zusammenarbeit mit Datenschutzbehörden entschieden haben, einschließlich Organisationen, die Personaldaten verarbeiten, müssen im Zusammenhang mit der Untersuchung und Bearbeitung von Beschwerden unmittelbar auf diese Behörden eingehen.

Organisationen sind verpflichtet, Ansprüche im Schiedsverfahren zu regeln und die in Anlage I aufgeführten Bedingungen einzuhalten, sofern eine Privatperson durch Benachrichtigung der betreffenden Organisation und entsprechend den Verfahren und Bedingungen nach Anlage I ein verbindliches Schiedsverfahren beantragt hat.

Im Zusammenhang mit einer Weitergabe ist eine dem Datenschutzschild angehörende Organisation für die Verarbeitung der personenbezogenen Daten, die sie im Rahmen des Datenschutzschilds erhält und anschließend an einen Dritten weitergibt, der in ihrem Auftrag und auf ihre Anweisung tätig ist, verantwortlich. Die dem Datenschutzschild angehörende Organisation bleibt nach den Grundsätzen haftbar, wenn ihr Beauftragter diese personenbezogenen Daten auf eine Art und Weise verarbeitet, die nicht im Einklang mit den Grundsätzen steht, es sei denn, sie weist nach, dass sie für das Ereignis, das den Schaden bewirkt hat, nicht verantwortlich ist.

Ist gegen eine Organisation eine Anordnung der FTC oder ein Gerichtsbeschluss wegen eines Verstoßes ergangen, macht die Organisation jene Teile eines der FTC vorgelegten Compliance- oder Sachstandsberichts, die den Datenschutzschild betreffen, öffentlich, soweit dies mit den Verpflichtungen zur Geheimhaltung im Einklang steht. Das Ministerium hat eine spezielle Kontaktstelle eingerichtet, an die sich Datenschutzbehörden bei Compliance-Problemen von dem Datenschutzschild angehörenden Organisationen wenden können. Die FTC wird Fälle der Missachtung der Grundsätze, die ihr vom Ministerium und Behörden der EU-Mitgliedstaaten zugeleitet wurden, vorrangig behandeln und vorbehaltlich der geltenden Geheimhaltungsvorschriften zeitnah mit den vorlegenden staatlichen Behörden Informationen zu diesen Fällen austauschen.

6.2.2 Zusatzgrundsätze zum Privacy Shield

1. Sensible Daten
2. Ausnahmen für den journalistischen Bereich
3. Hilfsweise Haftung
4. Due Diligence Prüfung und Wirtschaftsprüfung
5. Die Rolle der Datenschutzbehörden
6. Selbstzertifizierung
7. Anlassunabhängige Kontrolle
8. Auskunftsrecht
9. Personaldaten
10. Obligatorische Verträge bei Weitergabe
11. Beschwerdeverfahren und Durchsetzung
12. Wahlmöglichkeit – Zeitpunkt des Widerspruchs
13. Reisedaten
14. Arzneimittel und Medizinprodukte
15. Daten aus öffentlichen Registern und öffentlich zugängliche Daten

Die inhaltlichen Ausführungen sind unter Anhang 2 des Durchführungsbeschlusses 2016/1250 der Kommission zu finden und können ↗hier abgerufen werden.

6.2.3 Übersicht EU-Kommission Fact Sheet

Strenge Auflagen für Unternehmen und starke Durchsetzung

- Mehr Transparenz
- Wirksame Aufsichtsmechanismen, um sicherzustellen, dass Unternehmen die Regeln einhalten
- Sanktionen und Streichung von Privacy Shield - Liste
- Strengere Bedingungen für Weitergabe von Daten durch teilnehmende Unternehmen an Dritte

Wirksamer Rechtsschutz

Verschiedene Rechtsschutzmöglichkeiten

- Direkt beim Unternehmen: Unternehmen müssen innerhalb von 45 Tagen dem Betroffenen auf die Beschwerde antworten
- Alternative Streitbeilegung: Kostenlos
- Kontrolle durch EU-Datenschutzbehörde: Diese werden mit US-Handelsministerium und Federal Trade Commission zusammenarbeiten und dafür sorgen, dass Beschwerden von Bürgerinnen und Bürgern der EU nachgegangen und abgeholfen werden
- Schiedsverfahren durch Privacy Shield Panel: Als letzte Instanz

Schutzvorkehrungen bei Datenzugriff durch US-Behörden

- Zum ersten Mal schriftliche Zusicherungen, dass jeglicher Zugriff von US-Behörden auf personenbezogene Daten strengen Anforderungen und gerichtlichen Rechtsschutz unterliegt
- Zusicherungen, dass es keinen massenhaften Zugriff auf personenbezogene Daten ohne irgendeine Differenzierung, Einschränkung oder Ausnahme gibt
- Berichte von Unternehmen, wie oft sie von US-Behörden nach Zugang zu personenbezogenen Daten angefragt wurden
- Unabhängige Ombudsstelle, an die sich Bürger mit Rechtschutzbegehren, die den Bereich der nationalen Sicherheit betreffen, wenden können

Überprüfung des Angemessenheitsbeschlusses

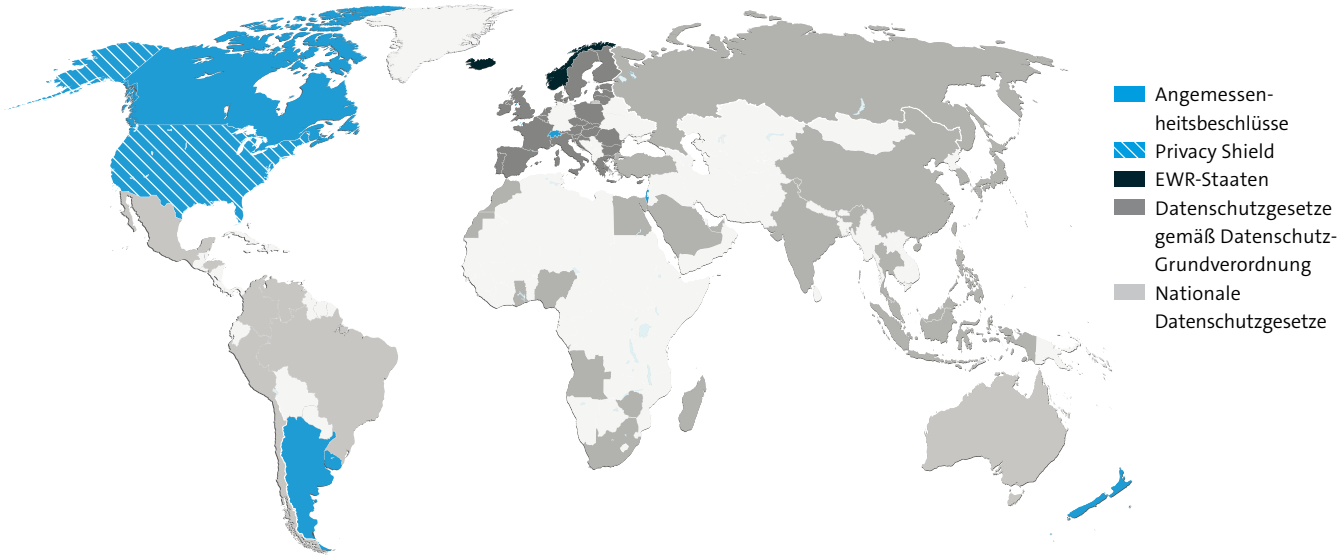
Jährliche gemeinsame Überprüfung

- Gemeinsame Überwachung der Funktionsweise des Privacy Shield und schriftlichen Zusicherungen der USA
- Von der EU-Kommission und dem US-Handelsministerium durchgeführt, an der ggf. auch Vertreter der Nachrichtendienste beteiligt werden können

Quelle: ↗Factsheets der EU-Kommission (2016)

6.3 Übersicht über den weltweiten Stand des Datenschutzes

6.3.1 Grafische Übersicht über den weltweiten Stand des Datenschutze



Hinweis: Laut EU-Kommission haben in den vergangenen Jahren weltweit immer mehr Länder neue Datenschutzvorschriften erlassen oder einen entsprechenden Prozess in Gang gesetzt. 2015 verfügten laut EU-Kommission insgesamt 109 Länder über Datenschutzgesetze, ein erheblicher Anstieg gegenüber den 76 Ländern, die Mitte 2011 gezählt wurden, ↗EU-Mitteilung (2017) 7, p. 8. In 2017 ist diese Zahl nochmal um 10 % auf 120 Länder angestiegen.[15]

Eine Übersicht zu nationalen Datenschutzgesetzen finden Sie auch auf dieser ↗Webseite von DLA Piper.

15 Greenleaf, Graham, Global data privacy laws (5th edition 2017) Stand 30 Juni 2017

6.3.2 Erläuterung zur grafischen Übersicht über den weltweiten Stand des Datenschutzes

Stand September 2017

Datenschutz-Gesetze gemäß EU-Datenschutzgrundverordnung	EWR – Staaten
Belgien	Island
Bulgarien	Liechtenstein
Dänemark	Norwegen
Estland	
Finnland	
Frankreich	
Griechenland	
Großbritannien	
Irland	
Italien	
Kroatien	
Lettland	
Litauen	
Luxemburg	
Malta	
Niederlande	
Österreich	
Polen	
Portugal	
Rumänien	
Schweden	
Slowakei	
Slowenien	
Spanien	
Tschechien	
Ungarn	
Zypern	

Angemessenes Datenschutzniveau durch EU-Kommission anerkannt	EU-US Privacy Shield Abkommen
Argentinien	Vereinigte Staaten
Andorra	
Guernsey	
Isle of Man	
Jersey	
Kanada	
Neuseeland	
Israel	
Schweiz	
Färöer Inseln	
Uruguay	

Datenschutzbehörden in Europa (außerhalb EWR)	Datenschutzbehörden International	
Albanien	Antigua und Barbuda	Mexiko
Armenien	Argentinien	Nepal
Bosnien und Herzegowina	Australien	Neuseeland
Georgien	Bahamas	Paraguay
Kosovo	Benin	Peru
Mazedonien	Brasilien	Philippinen
Moldawien	Burkina Faso	São Tomé und Príncipe
Montenego	Chile	Senegal
Russland	Costa Rica	Simbabwe
Schweiz	Dom. Rep.	Singapur
Serbien	Dubai	Südafrika
Türkei	Elfenbeinküste	Südkorea
Ukraine	Equatorialguinea	Senegal
	Gabon	St. Lucia
	Hong Kong	Taiwan
	Israel	Thailand
	Japan	Trinidad und Tobago
	Jemen	Tunesien
	Hong Kong	Uruguay
	Kanada	USA
	Kap Verde	
	Kasachstan	
	Kirgisistan	
	Kolumbien	
	Lesotho	
	Costa Rica	
	Macao	
	Malaysia	
	Malawi	
	Mali	
	Marokko	
	Mauritius	

Quelle: International Conference of Data Protection & Privacy Commissioners (↗ICDPPC). Auch Greenleaf gibt eine gute Übersicht in den »Global Tables of data Privacy Laws and Bills (5th edition 2017)«.

Nationale Datenschutz-Gesetze [16]

Abu Dhabi (2015)
Albanien (1999/2012)
Angola (2011)
Antigua & Barbuda (2013)
Argentinien (2000)
Armenien (2002/2015)
Äquatorialguinea (2016)
Aruba (2011)
Australien (1988/2012)
Azerbaijan (1998/2010)
Benin (2009)
Bahamas (2003)
Bermuda (2016)
Bosnien Herzegowina (2001)
Burkina Faso (2004)
Chad (2015)
Chile (1999/2012)
Costa Rica (2011/2013)
Curacao (2010)
Dominikanische Republik (2013)
Dubai (2007)
Elfenbeinküste (2013)
Equatorialguinea (2016)
Gabon (2011)
Georgien (2012)
Ghana (2012)
Hong Kong (1995/2012)
Indien (2011)
Indonesien (2016)
Israel (1981)
Japan (2003/2015)
Jemen (2012)
Kanada (1983/2002)
Kap Verde (2001)
Karibische Niederlande (2010)
Kasachstan (2013/2015)
Katar (2016)
Kirgistan (2008)
Kolumbien (2008/2012)
Kosovo (2010)
Lesotho (2011)
Macao (2006)
Madagaskar (2015)
Malawi (2016)
Malaysia (2010/2013)
Mali (2013)
Marokko (2009)
Mauritius (2004)
Mazedonien(1994/2005)
Mexiko (2010/2016)
Moldawien (2007)
Montenegro (1998/2008)
Nepal (2007)
Neuseeland (1993/2010)
Nicaragua (2012)
Norwegen (1978/2010)
Paraguay (2002)
Peru (2011)
Philippinen (2012)
Russland (2006/2011 und 2014)
São Tomé und Príncipe (2016)
Schweiz (1992/2006)
Senegal (2008)
Serbien (2008)
Seychellen (2003)
Simbabwe (2002)
Singapur (2012)
St. Lucia (2011)
St. Maartens (2010)
St. Vincent & Grenadines (2003)
Südafrika (2013)
Südkorea (1994/2015)
Taiwan (1995/2010)
Thailand (1997)
Trinidad und Tobago (2011)
Tschad (2015)
Tunesien (2004)
Ukraine (2011/2015)
Uruguay (2008)
Vietnam (2010)
Vereinigte Staaten (1994)

Hinweis: Hier werden nur die Länder aufgeführt, die ein Datenschutzgesetz erlassen haben. Dies heißt nicht, dass es in den anderen Ländern keine datenschutzrechtlichen Regelungen gibt.

16 Greenleaf, Graham, Global data privacy laws (5th edition 2017) Stand 30 Juni 2017.

6.4 Übersicht über die rechtlichen Mögklichkeiten der Übermittlung personenbezogener Daten in Drittländer

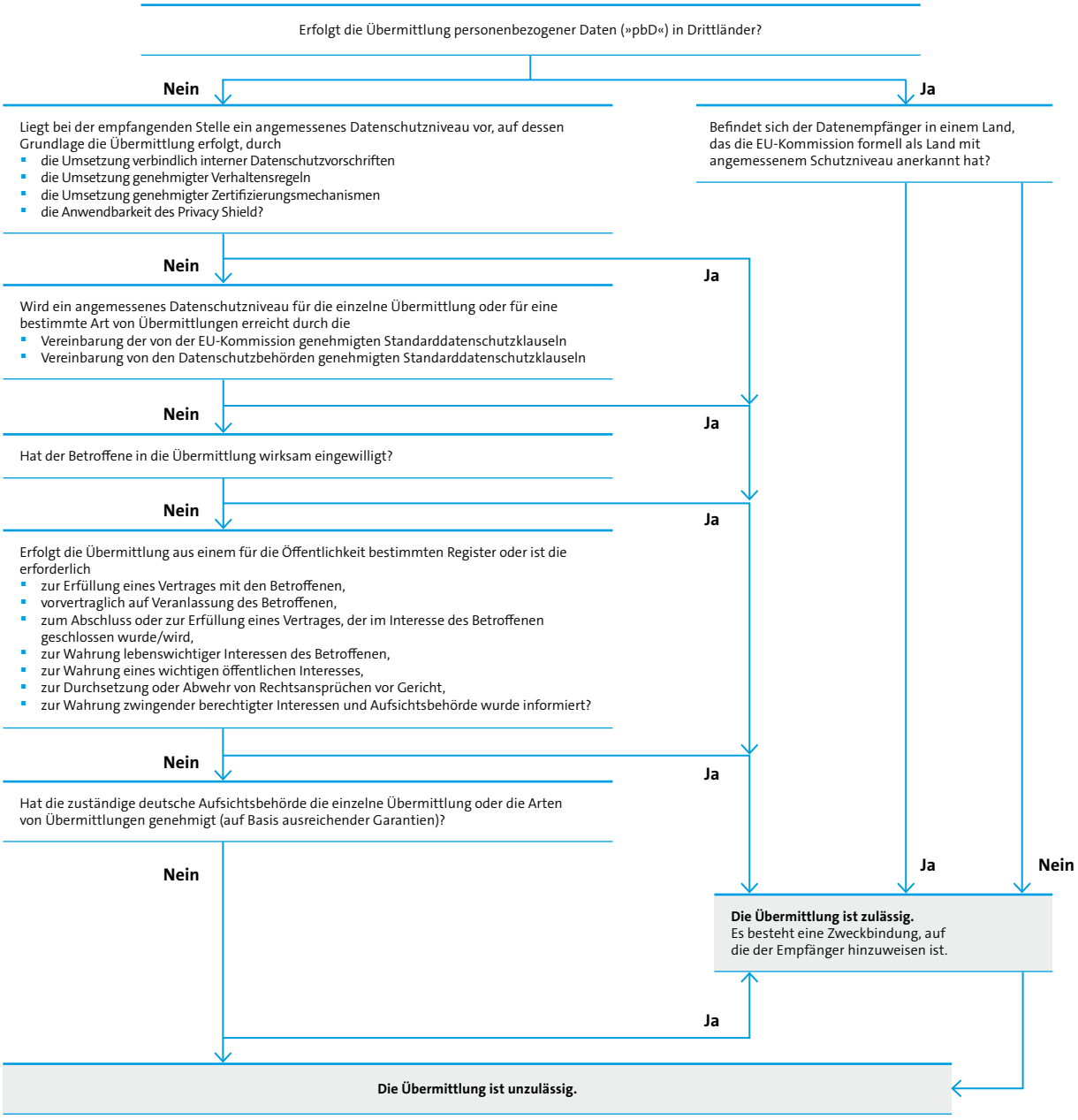
	»Art«	Geltungsbereich	Abschluss	Pb Daten	Aufsichtsbehörde	Bemerkungen
Einwilligung (Art. 49 Abs. 1 lit. a)	Einseitige, empfangsbedürftige Einwilligungserklärung	Individuell; zwischen betroffener Person und Verantwortlichen	Durch Abgabe der entsprechenden Willenserklärung seitens des Einwilligenden	Grundsätzlich die autorisierten pb Daten des Betroffenen; Umfang im Rahmen der gesetzlichen Möglichkeiten, der guten Sitten u. des vorgesehenen Zwecks	Keine Mitwirkung erforderlich	Die betroffene Person muss über die für sie möglicherweise bestehenden Risiken unterrichtet worden sein, und sie muss ihre Einwilligung ausdrücklich abgegeben haben
Datenübermittlung ist zur Erfüllung des Vertrages o. zur Durchführung vorvertraglicher Maßnahmen erforderlich (Art. 49 Abs. 1 lit. b)	Vertrag o. vertragsähnliche Beziehung zwischen Verantwortlichen und betroffener Person	Individuell; zwischen betroffener Person und Verantwortlichen	Durch Abgabe der entsprechenden Willenserklärungen vom Verantwortlichen und der betroffenen Person	Grundsätzlich die pb Daten des Betroffenen, die für die Durchführung des Vertrages erforderlich sind	Keine Mitwirkung erforderlich	Vertragsbeispiele: Hotelreservierung im Ausland; Arbeitsvertrag mit ausländischem Arbeitgeber; Warenbestellung (auch online) im Ausland
Datenübermittlung ist zum Abschluss o. zur Erfüllung eines im Interesse der betroffenen Person geschlossenen Vertrags erforderlich (Art. 49 Abs. 1 lit. c)	Vertrag zwischen Verantwortlichen und einem Dritten	Individuell; zwischen Verantwortlichen und einem Dritten	Durch Abgabe der entsprechenden Willenserklärungen vom Verantwortlichen und Dritten	Grundsätzlich die pb Daten des Betroffenen, die für die Durchführung des Vertrages erforderlich sind	Keine Mitwirkung erforderlich	Vertragsbeispiele: Übermittlung Daten Arbeitnehmer für Mitarbeiterversicherung an ausländische Versicherungsgesellschaft
Andere Ausnahmen (Art. 49 Abs.1 lit d –f)	Anderer Ausnahmetatbestand	Begrenzt auf den Sachverhalt der Ausnahmeregelung	Prüfung erforderlich, ob die Voraussetzungen des Ausnahmetatbestands vorliegen	Mitarbeiter-, Kunden-, Nichtkunden, - Interessenten und Lieferantendaten, soweit für die Übermittlung im Rahmen der Ausnahmeregelung erforderlich	Keine Mitwirkung erforderlich	z. B. Wahrung eines wichtigen öffentlichen Interesses; Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht; Wah rung lebenswichtiger Interessen
Drittländer mit durch die EU Kommission festgestelltem angemessenen Datenschutzniveau (Art. 45)	Entscheidung gemäß Art. 45 (EU-Kommissionsentscheidung)	Gilt für alle Empfänger im entscheidungsgegenständlichen Drittland	n. a.	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten	Keine Mitwirkung erforderlich	Kommissionsentscheidung liegen derzeit vor für: Argentinien, Andorra, Guernsey, Isle of Man, Jersey, Kanada, Neuseeland, Israel, Schweiz, Färöer, Uruguay

	»Art«	Geltungsbereich	Abschluss	Pb Daten	Aufsichtsbehörde	Bemerkungen
Individuelle Vertragsklauseln (Art. 46 Abs. 3 lit. a)	Vertragliche, verbindliche Regelung zwischen den Parteien (auch mehrere, auch Unterauftragsnehmer) über den Umgang mit personenbezogenen Daten	Zwischen den Vertragsparteien (auch mehr als 2) z. B. Datenexporteur (Verantwortlicher, Auftragsverarbeiter) und Datenimporteur (Verantwortlicher, Auftragsverarbeiter)	Durch Abgabe der entsprechenden Willenserklärungen zwischen den vertragsschließenden Parteien	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten und Lieferantendaten soweit sie Gegenstand des individuellen Datenschutzvertrages sein sollen	Genehmigung einzelner Daten-übermittlungen oder bestimmter Arten von Übermittlungen pb Daten durch Aufsichtsbehörde gem. Art. 46 Abs. 3	Flexibel; (z. B. Anpassung an Besonderheiten einer bestimmten Branche), je nach Umfang auch zeitaufwendig wesentlichen Datenschutzgarantien der DS-GVO sowie für die betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe müssen eingeräumt werden.
Vertrag auf Basis der Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten (auch an Auftragsverarbeiter) (Art. 46 Abs. 2 lit. c und lit. d)	Vertrag zwischen Datenexporteur und dem Datenimporteur auf Basis der EU-Kommisionsentscheidung zu den Standarddatenschutzklauseln oder den genehmigten Standarddatenschutzklauseln der Aufsichtsbehörden	Zwischen atenimpoteur(en) in einem Drittland und Exporteur(en) mit Sitz in der EU.	Durch Abgabe der entsprechenden Willenserklärung zwischen den vertragsschließenden Parteien.	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten und Lieferantendaten soweit sie Gegenstand des individuellen Datenschutzvertrages sein sollen	Bei unverändertem Abschluss des Vertrages keine Genehmigung erforderlich	Schnell umsetzbar. Einfach. Für große internationale Unternehmsverbünde wohl unpraktikabel, da umfangreiches Vertragsmanagement erforderlich.
Binding Corporate Rules (»Verbindliche unternehmensinterne Vorschriften) (Art. 46 Abs. 2 lit.b iVM Art. 47)	Verbindliche Unternehmensregelungen für Teile oder die Gesamtheit eines multinationalen Unternehmensverbundes (Konzern) oder Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben (z. B. bestimmte Branche)	Die Teile des Konzerns, für die Unternehmensregelung (BCR) verbindlich sind	Verbindliche, interne Anweisung durch die führende Gesellschaft	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten und Lieferantendaten soweit sie Gegenstand des individuellen Datenschutzvertrages sein sollen	Nach Abschluss keine (zusätzlichen) weiteren aufsichtsbehördlichen Genehmigungen notwendig	
Genehmigte Verhaltensregeln (Codes of Conduct) (Art. 46 Abs. 2 lit. e)	Vereinbarung Verantwortlichen oder Auftragsverarbeitern über verbindliche Verhaltensregeln zum Datenschutz	Datenverkehr pb Daten zwischen Datenexporteuren mit Sitz in der EU und an CoC teilnehmenden Unternehmen (Datenimporteur)	Beitritt der Unternehmen zu CoC durch rechtsverbindliche und durchsetzbare Verpflichtung zur Befolgung der in den Verhaltensregeln enthaltenen Garantien	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Liefe-rantendaten im Rahmen der Registrierung	Nach Zustimmung der zuständigen Aufsichtsbehörde und Gültigkeitserklärung der EU-Kommission keine weiteren Genehmigungen notwendig	

	»Art«	Geltungsbereich	Abschluss	Pb Daten	Aufsichtsbehörde	Bemerkungen
Genehmigte Zertifizierungsmechanismen (Art. 46 Abs. 2 lit. f i. V.m Art.42)	Rechtsverbindliche und durchsetzbare Verpflichtungen zur Befolgung geeigneter Garantien durch den Verantwortlichen oder Auftragsvearbeiter	Datenverkehr pb Daten zwischen Datenexporteuren mit Sitz in der EU und der von Zertifizierungsstellen oder Aufsichtsbehörden zertifizierten Unternehmen (Datenimporteur)	Datenexporteure und -importeure wurden gem. den Zertifizierungskriterien durch die Zertifizierungsstellen oder durch die zuständige Aufsichtsbehörde zertifiziert	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten im Rahmen der Registrierung	Nach Zertifizierung keine weiteren Genehmigungen notwendig	
Privacy Shield	Vereinbarung zwischen den USA und der EU über verbindliche Verhaltensregeln zum Datenschutz für US-amerikanische Unternehmen	Datenverkehr pb Daten zwischen Datenexporteuren mit Sitz in der EU und an Privacy Shield teilnehmenden Unternehmen (Datenimporteur) in den USA	Beitritt der US-Unternehmens zu dem Privacy Shield Programm durch Beitrittserklärung, Registrierung auf einer Internet- Webseite und Veröffentlichung bestimmter Informationen; Datenexporteur muss in der EU seinen Sitz haben	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten im Rahmen der Registrierung	Keine Mitwirkung erforderlich; ggf. Hinweis des Übermittlers auf Teilnahme des Datenempfängers an dem Privacy-Shield-Programm	Jährliche Überprüfung
Nichts tun	Keine Regelung implementieren	n.a.	n.a.	n.a.	n.a.	Hohes Risiko für die Verantwortlichen (Bußgeld/ Haftstrafe) und das Unternehmen (Schadensersatz/Risiko der Untersagung der Geschäftstätigkeit des EDV-Betriebs/neg. Auswirkungen auf Image, Umsatz, Ertrag, Shareholder-Value

Quelle: AK Datenschutz | Stand September 2017

6.5 Möglichkeiten der Datenübermittlung



7 Weiterführende Links und Literatur

7 Weiterführende Links und Literatur

Urteile

EuGH, Urteil vom 24.11.2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado, C-468/10 und C-469/10, EU:C: 2011:777.

EuGH, Urteil vom 1.10.2015, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, EU:C:2015:639.

EuGH, Urteil vom 6.10.2015, Schrems v DPC Irland, C-362/24, EU:C:2015:650.

Irish High Court, Data Protection Commissioner v. Facebook Ireland Limited & Maximilian Schrems, Az. 2016/4809P.

La Quadrature du Net and others v Commission, Case T-738/16. Digital Rights Ireland v Commission, Case T-670/16.

Aufsätze

Schmitz, Barbara/v. Dall'Armi, Jonas, Standardvertragsklauseln – heute und morgen – Eine Alternative für den Datentransfer in Drittländer?, ZD 2016, 217ff.

Drewes, Stefan/Monreal, Manfred, Grenzenlose Auftragsdatenverarbeitung, PinG 2014, 143 ff.

Greenleaf, Graham, Global Tables of Data Privacy Laws, Privacy Laws & Business International Report 2017, 14–26. Kostenloser Download unter: ↗https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992986.

Datenschutzaufsichtsbehörden

↗Arbeitspapiere der Art. 29-Datenschutzgruppe

↗Entschließungen des Düsseldorfer Kreises
(Oberste Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich)
Abgestimmte Positionen der Aufsichtsbehörden in der AG »Internationaler Datenverkehr» am 12./13. Februar 2007, Seite 2, II.2.

↗International Conference of Data Protection & Privacy Commissioners

Weitere hilfreiche Links

↗DLA Piper: Data Protection Laws of the Worlds.

Centrum für europäische Politik, Datenübermittlung in Drittländer, Analyse EU-Mitteilung COM (2017)7, Kostenloser Download unter: ↗http://www.cep.eu/fileadmin/user_upload/cep.eu/Analysen/COM_2017_7_Datenuebermittlung/cepAnalyse_COM_2017__7_Datenuebermittlung_in_Drittlaender.pdf

Bitkom vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft, davon gut 1.700 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 400 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom